Lotus

# Sametime

Gruppenarbeit in Echtzeit, die für den Einsatz in Unternehmen bestens geeignet ist

1.5
RELEASE

## Administratorhandbuch

## Information zu Copyright und Warenzeichen



**Warenzeichen**



**Garantieausschluß; keine Garantie**

# Kapitel 01: Einführung in Sametime

## Was ist Sametime?

Lotus® Sametime™ verbindet Web-Server-, Lotus Notes®-, T.120 Datenkonferenz- und Online-Awareness -Technologie. Es ermöglicht dadurch Lotus Notes- und Web-Browser Clients die Teilnahme an interaktiven Online-Besprechungen, direktem Nachrichtenaustausch und Gruppendiskussionen. Sametime verbessert den Arbeitsplatz, indem leistungsfähige Echtzeitwerkzeuge auf allen Desktops der Sametime Community installiert werden.

Sametime besteht aus den folgenden Elementen:

**Sametime Server** - Der Sametime Server bietet folgende Dienste, um für Web-Browser und Notes™ Clients der Sametime Community Online-Awareness, Chat-Möglichkeiten und gemeinsame Nutzung von Anwendungen zu garantieren.

- Community Service
- Meeting Service
- Web Application Service
- Domino Application Service

**Sametime Connect** - Die Client-Anwendung Sametime Connect ermöglicht Benutzern, eine Online-Liste aller Kollegen zu führen und diesen Nachrichten in Echtzeit zu senden. Die Benutzer müssen die Anwendung Sametime Connect™ vom Sametime Server herunterladen, auf ihrem Computer installieren und von dort aus verwenden.

Benutzer können mit anderen Online-Benutzern von Sametime Connect aus auch nicht geplante Besprechungen mit gemeinsam genutzter Anwendung initiieren.

**Sametime Schablonen und Anwendungen** - Der Sametime Server enthält Sametime Diskussionsbeispiele, E-Mail-Muster und Musterdokumente für Bibliotheksschablonen, die Echtzeit-Zusammenarbeit für weitverbreitete Lotus Domino™ Anwendungen ermöglichen. Der Server enthält außerdem das Sametime Online-Besprechungszentrum, einen zentralen Treffpunkt, wo Mitglieder der Sametime Community Informationen und Anwendungen in Echtzeit-Online-Besprechungen austauschen können. Web-Browser Clients können auf die Diskussions- und Online-Besprechungszentrums-Anwendungen auch dann zugreifen, wenn ihr Unternehmen keine Domino Produkte verwendet.

Ein Administrator verwendet das Sametime Administrationswerkzeug, um den Sametime Server zu verwalten. Das Sametime Administrationswerkzeug ist über den Web Browser erhältlich, nachdem Sie die Sametime Installation bzw. das Setup beendet haben (im Sametime Installationshandbuch beschrieben).

Verwandte Themen anzeigen
Unterstützte Umgebungen für Sametime

## Unterstützte Umgebungen für Sametime

Sametime kann entweder in einer schon bestehenden Domino Domäne oder in einer Web-Umgebung ohne Domino Server genutzt werden. Während der Installation können Sie die Umgebung für Sametime auswählen.

- **Sametime in einer Domino Umgebung** - Wenn Ihr Unternehmen Domino Server verwendet, können ein oder mehrere Sametime Server in einer Domino Umgebung installiert werden. Ein Sametime Server korrespondiert mit dem Domino Server in einer Domino Domäne.

  Sametime muß auf einem Windows NT Server installiert werden. Sie können Sametime auf einem eigenen Server ohne Domino oder auf einem Server installieren, auf dem Domino bereits installiert ist.

  Bei der Installation in einer Domino Umgebung, in der Domino Server mit einer älteren Domino Server Version als 4.6.5 laufen, wird das Adreßbuch auf dem Server geändert, auf dem Sametime läuft. Unabhängig davon, ob Sie Sametime auf einem eigenen Server oder einem Server mit Domino installieren, sollten Sie verhindern, daß das Adreßbuch vom Sametime Server auf die Domino Server in der Domäne repliziert wird. Installationsanleitungen finden Sie im *Sametime Installationshandbuch*.

  Bei der Installation in einer Domino Umgebung, in der Domino Server mit der Domino Server Version 4.6.5 oder höher laufen, werden alle von Sametime verlangten Adreßbuch-Designänderungen in das Domino Release integriert. Die Replizierung des Adreßbuchs von einem Server, auf dem Sametime läuft, auf die Domino Server sollte problemlos verlaufen. Installationsanleitungen finden Sie im *Sametime Installationshandbuch*.

Wenn Sametime in einer Domino Umgebung installiert wird, korrespondiert es mit den Verzeichnis-, Sicherheits- und Replizierungsfunktionen von Domino. Diskussionsdatenbanken können mit Sametime Funktionen versehen werden, wie z. B. Online-Awareness, direktem Nachrichtenaustausch und Gruppen-Chat. E-Mail-Muster und Datenbanken sind ebenfalls beigefügt, um zu demonstrieren, wie diese Sametime Funktionen in E-Mail-Anwendungen und Anwendungen für Dokumentbibliotheken integriert werden können. Lotus Notes und Web-Browser Clients können mit demselben Sametime Server in Verbindung treten, wenn dieser als Teil der Domino Domäne verwendet wird. Notes und Browser Clients können auf die Online-Besprechungszentrums-Anwendung zugreifen, um Informationen und Anwendungen in Echtzeit-Online-Besprechungen auszutauschen.

Wenn Sie mehr als einen Sametime Server in einer Domino Domäne installieren, kann jeder Domino Server der Domäne mit jedem anderen Sametime Server kommunizieren. Die Sametime Server können außerdem untereinander kommunizieren. Wenn Sie mehrere Sametime Server verwenden, müssen Sie diese aktivieren, damit sie als einzelne Community arbeiten. Weitere Informationen hierzu finden Sie unter Verwenden mehrerer Sametime Server.

- **Sametime in einer reinen Web-Umgebung** - Wenn Ihr Unternehmen keine Domino Server verwendet, können Sie den Sametime Server als reinen Web-Server nutzen. Web-Browser können auf das Besprechungszentrum auf dem Sametime Server zugreifen, um Informationen und Anwendungen in Online-Konferenzen in Echtzeit gemeinsam zu nutzen. Diese Benutzer können auch auf eine Diskussionsanwendung zugreifen, die Online-Awareness, direkten Nachrichtenaustausch und Gruppen-Chat-Funktionen beinhaltet.

  Wie Sie Sametime auf einem reinen Web-Server installieren, entnehmen Sie bitte dem Sametime Installationshandbuch.

Den Sametime Connect Client lädt jeder Benutzer der Sametime Community vom Sametime Server herunter. Sametime Connect ist eine separate Windows 95/NT-Anwendung, die auf dem Computer jedes Benutzers läuft. Sametime Connect können Sie in einer Domino oder einer reinen Web-Umgebung betreiben.

## Info über die Sametime Community

Die Sametime Community besteht aus der Benutzergruppe, die Zugriff auf den Sametime Server und auf den Sametime Connect Client hat. Die Sametime Community läßt sich am besten anhand der beiden Umgebungen erläutern, die von Sametime unterstützt werden.

- **Sametime Community in einer Domino Umgebung** - Die Sametime Community wird durch die Benutzer im Öffentlichen Adreßbuch definiert.

  Die Benutzer im Öffentlichen Adreßbuch stellen die Sametime Community dar und haben untereinander Leistungsmerkmale wie direkten Nachrichtenaustausch, Online-Awareness und gemeinsame Nutzung von Anwendungen. Authentifizierung für Lotus Notes und Web-Browser-Clients in der Domino Domäne funktioniert auf einem Sametime Server genauso wie auf einem Domino Server. Um Mitglied der Sametime Community zu werden, muß ein Lotus Notes Benutzer registrierter Benutzer in der Domino Domäne sein. Web-Browser-Benutzer müssen über Zugriff auf den Sametime Server und ein Personendokument mit Internet-Kennwort im Adreßbuch verfügen. Alle Benutzer müssen ein Internet-Kennwort besitzen, um auf Sametime Connect zuzugreifen.

  Wenn Sie mehrere Sametime Server in einer Domino Umgebung installieren, können Sie die Sametime Connect Server als einzelne Community aktivieren. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server.

- **Sametime Community in einer reinen Web-Umgebung** - Wenn Sie den Sametime Server in einer reinen Web-Umgebung verwenden, können Sie die Sametime Community erweitern, indem Sie im Verlauf der Installation bzw. des Setups dem Sametime Adreßbuch neue Benutzer hinzufügen. Die Benutzer der Community genießen Leistungsmerkmale wie direkten Nachrichtenaustausch, Online-Awareness und gemeinsame Nutzung von Anwendungen. Ein Benutzer kann Mitglied der Community werden, indem er mit Hilfe eines Web-Browsers über Zugriff auf den Sametime Server und ein Personendokument mit Internet-Kennwort im Sametime Adreßbuch verfügt.

  Wenn Sametime in einer reinen Web-Umgebung installiert ist, verwenden Sie das Sametime Administrationswerkzeug, um die Sametime Community zu füllen. Sametime umfaßt auch eine Funktion zur Selbstregistrierung, über die sich Benutzer selbst in das Sametime Adreßbuch aufnehmen können. Weitere Informationen finden Sie unter Verwenden der Selbstregistrierung.

## Online-Awareness und sofortige Nachricht

Online-Awareness bezieht sich auf die Möglichkeit der Benutzer der Sametime Community, andere Benutzer der Sametime Community, die online sind, zu "sehen". Im allgemeinen besteht die Online-Awareness aus einer Liste von Benutzern, die in der Sametime Client-Anwendung angezeigt wird. Sametime-aktivierte Datenbanken können auch die Listen "Wer ist anwesend" und "Wer ist online" enthalten, die Endbenutzern Online-Mitglieder der Sametime Community anzeigen. Gewöhnlich werden Benutzer, die online sind, in diesen Listen grün dargestellt.

Ein Benutzer kann einen Chat beginnen, indem er eine direkte Nachricht an einen anderen Benutzer schickt, der online ist. Es können dann weitere Benutzer zum Chat eingeladen werden, so daß Mehrpersonen-Chats entstehen.

Online-Awareness, direkter Nachrichtenaustausch und Chat-Möglichkeiten werden von folgenden Sametime Komponenten unterstützt:

- Sametime Connect
- Sametime-aktivierte Datenbanken und Anwendungen
- Community Services

## Sametime Connect

Jeder Benutzer der Sametime Community sollte das Sametime Client Paket vom Sametime Server herunterladen und installieren. Dieses Paket enthält den Sametime Connect Client, der als eigenständige Windows 95/NT-Anwendung auf den Computern der Benutzer läuft.

Jeder Benutzer kann die Namen anderer Benutzer der Community zum Sametime Connect Client hinzufügen. Sametime Connect enthält eine Funktion "Benutzer hinzufügen", die es ermöglicht, die Namensliste des Sametime Adreßbuchs zu durchsuchen und einzelne Benutzer oder Benutzergruppen hinzuzufügen. Die Namen der Benutzer, die gerade online sind, erscheinen in Grün auf demselben Sametime Connect Client. Jeder Benutzer kann an jeden anderen Benutzer, der online ist, eine direkte Nachricht senden und außerdem andere Benutzer zu einem Mehrpersonen-Chat einladen. Ein Benutzer ist dann online, wenn er Sametime Connect startet oder wenn er sich in einer Sametime Anwendung mit Online-Awareness und Chat-Möglichkeiten befindet.

Sametime Connect Online-Awareness und Chat-Möglichkeiten werden von Community Services auf dem Sametime Server unterstützt. Wenn ein Benutzer den Sametime Connect Client öffnet, muß der Client eine Verbindung zum Sametime Community Server aufbauen. Der Sametime Connect Client umfaßt Sametime Verbindungseinstellungen, die den Client-Verbindungsprozeß steuern. Mit Hilfe dieser Einstellungen kann der Sametime Connect Client direkt oder über einen Proxy-Server eine Verbindung zum Community Server aufbauen.

Verbindungen von Sametime Connect Clients werden durch Anschlüsse auf dem Sametime Server unterstützt. Weitere Informationen über diese Verbindungen finden Sie unter Verbindung mit dem Community Server.

Sie können auch mit anderen Online-Benutzern von Sametime Connect aus auch nicht geplante Besprechungen mit gemeinsam genutzter Anwendung initiieren eine nicht geplante Besprechung mit gemeinsam genutzter Anwendung. Die Sametime Connect Funktion für gemeinsam genutzte Anwendungen wird von den Meeting Services auf dem Sametime Server unterstützt.

Der Sametime Connect Client umfaßt Privacy-Funktionen, die einzelne Benutzer daran hindern, zu sehen, wann Sie online sind oder Sie dann zu kontaktieren. Einträge für die Sametime Connect Privacy-Funktionen werden in der Privacy-Datenbank (VPUSERINFO.NSF) auf dem Sametime Server unterhalten.

Verwandte Themen anzeigen
Sametime-aktivierte Schablonen und Anwendungen
Community Services

## Sametime-aktivierte Schablonen und Anwendungen

Sametime Server, die in einer Domino Umgebung installiert werden, enthalten Sametime Diskussionen, E-Mail-Muster und Anwendungen für Muster-Dokumentbibliotheken, die Online-Awareness und Echtzeit-Diskussionsmöglichkeiten umfassen. Benutzer können sich in der Sametime Community mit Hilfe des Sametime Connect Clients anmelden oder indem Sie ein Dokument oder eine E-Mail in einer Sametime Anwendung öffnen. Diese Sametime Anwendungen zeigen die Listen "Wer ist anwesend" und "Wer ist online" an, die von Community Services auf dem Sametime Server erstellt wurden. Das Fenster "Wer ist online" listet die Benutzer auf, die bei der Sametime Community angemeldet sind. Das Fenster "Wer ist anwesend" listet die Benutzer auf, die dasselbe Dokument in der Sametime Anwendung geöffnet haben.

Wenn ein Benutzer ein Dokument der Sametime Diskussionsdatenbank ansieht, kann er die Option "Wer ist anwesend" auswählen, um eine Liste der Online-Benutzer zu sehen, die momentan das Dokument ansehen. Indem er die Option "An Chat hier teilnehmen" auswählt, kann der Benutzer mit anderen an einer Echtzeit-Diskussion über das Dokument, das diese gerade ansehen, teilnehmen. Sie können die Diskussionsschablone verwenden, um andere Diskussionsdatenbanken für Sametime zu erstellen. Ebenso können Sie den Entwurf bestehender Diskussions-Datenbanken in der Domino Domäne ersetzen, um diesen Datenbanken Online-Awareness und Diskussionsleistungsmerkmale hinzuzufügen.

Der Benutzer kann auch eine nicht geplante Besprechung mit gemeinsam genutzter Anwendung über die Funktionen "Wer ist anwesend" und "Wer ist online" in Sametime-aktivierten Datenbanken initiieren. Diese Besprechungen werden von Meeting Services auf dem Sametime Server unterstützt.

Die Dokumentbibliothek und E-Mail-Datenbanken sind Beispiele dafür, wie Sie Sametime Funktionen in neue Anwendungen integrieren können. Lotus Notes Designer können über die Datenbank "Tools and Utilities" weitere Informationen über die Entwicklung von Sametime Anwendungen erhalten.

Eine Sametime-aktivierte Datenbank kann auf einem anderen Server in der Domino Domäne eingesetzt werden. Weitere Informationen hierzu finden Sie unter Verwenden von Sametime-aktivierten Datenbanken.

Verwandte Themen anzeigen

- Sametime Connect
- Community Services
- Einsetzen Sametime-aktivierter Datenbanken

## Community Services

Die Komponente Sametime Community Server unterstützt die Community Services. Online-Awareness, direkter Nachrichtenaustausch und Mehrpersonen-Chat-Konferenzen verwenden Community Services auf dem Sametime Server. Die Community Services unterstützen:

- Direkte Client-Verbindungen mit dem Sametime Server. Sie können die Anzahl der Verbindungen zu den Community Services begrenzen. Auf Computern mit anspruchsvollen Verarbeitungsfähigkeiten werden bis zu 20000 TCP/IP-Verbindungen zu den Community Services unterstützt (z. B. Doppelprozessoren, 1 MB-Netzwerkkarte und 512 MB RAM). In der Regel werden 8000 TCP/IP-Verbindungen auf Computern empfohlen, die den System-Mindestanforderungen genügen. Clients stellen eine Verbindung zu den Community Services standardmäßig über Anschluß 1533 her.
- Verbindungen von Clients, die über einen HTTP-, HTTPS- oder SOCKS-Proxy auf das Internet zugreifen.
- Client-Login Anfragen für Sametime Connect und Sametime-aktivierte Datenbanken mit Online-Awareness und Chat-Fähigkeiten. Jeder Benutzer der Sametime Community benötigt ein Personendokument im Sametime Adreßbuch, das ein Internet-Kennwort enthält, um sich bei Sametime Connect anzumelden.
- Sametime Adreßbuch durchsuchen. Benutzer durchsuchen das Sametime Adreßbuch, um in Sametime Connect Namen und Gruppen zur Connect Liste hinzuzufügen.

  Wenn Sie Sametime in einer Domino Domäne installieren, werden überlappende Adreßbücher und Master Adreßbücher (Adreßverzeichnishilfe oder Adreßbuchhilfe) unterstützt, wenn Sie Benutzer oder Gruppen suchen.

- Die Funktionen "Wer ist online" und "Wer ist anwesend" in Sametime Connect und Sametime Anwendungen und Datenbanken.
- Eintragen von Ereignissen der Community Services im Sametime Protokoll (STLOG.NSF).

Auf der Seite "Netzwerk- und Sicherheits-Administration" können Sie die Anschluß-Einstellungen für die Community Services konfigurieren, die über das Sametime Administrationswerkzeug zur Verfügung stehen. Informationen über andere Administrationseinstellungen der Community Services finden Sie unter Administrationseinstellungen der Community Services.

Verwandte Themen anzeigen
Sametime Connect
Sametime-aktivierte Schablonen und Anwendungen

## Online-Besprechungen

Sametime Benutzer können Online-Besprechungen im Besprechungszentrum auf dem Sametime Server einrichten und an ihnen teilnehmen. Online-Besprechungen ermöglichen mehreren Benutzern der Sametime Community, durch gemeinsame Nutzung von Anwendungen oder einer Pinnwand in Echtzeit zusammenzuarbeiten. Sie können auch eine sofortige (oder nicht geplante) Besprechung mit gemeinsam genutzter Anwendung vom Sametime Client aus starten. Online-Besprechungen werden von den folgenden Sametime Komponenten unterstützt:

- Sametime Online-Besprechungen
- Sametime Connect Funktion für gemeinsam genutzte Anwendungen
- Meeting Services

Verwandte Themen anzeigen
Sametime Online-Besprechungszentrum

## Sametime Online-Besprechungszentrum

Das Besprechungszentrum ist eine Anwendung (STCONF.NSF) auf dem Sametime Server, auf die entweder über Notes Clients oder über Web-Browser zugegriffen werden kann. Das Besprechungszentrum ermöglicht Arbeitskollegen, die an verschiedenen Orten arbeiten, über die gemeinsame Nutzung von Anwendungen oder Pinnwandbesprechungen zusammenzuarbeiten.

In einer Besprechung mit gemeinsam genutzten Anwendungen kann ein Benutzer (der Teilnehmer, der die Anwendung freigibt) eine Anwendung auf seinem Computer mit anderen Teilnehmern der Besprechung teilen. Teilnehmer der Besprechung können die Anwendung auf dem Computer des Teilnehmers, der die Besprechung freigibt, verwenden, obwohl sie sich an einem anderen geographischen Ort befinden. Mit Hilfe dieser Technologie können Kollegen, die an verschiedenen Orten arbeiten, in derselben Anwendung in Echtzeit zusammenarbeiten.

Eine Pinnwand-Besprechung gleicht einer Präsentation. Ein Teilnehmer präsentiert Bilder auf einer gemeinsam genutzten Pinnwand. Die anderen Teilnehmer der Besprechung können am besprochenen Bild zeichnen oder Textnachrichten eingeben, um schriftliche Anmerkungen zum Bild beizutragen.

Sobald ein Benutzer eine Online-Besprechung initiiert oder an einer Online-Besprechung teilnimmt werden die Java-Applets für "Gemeinsame Nutzung von Anwendungen" und "Pinnwandbetrachter" vom Sametime Server auf den Client heruntergeladen. Clients verwenden diese Applets, um an einer Online-Besprechung teilzunehmen. Um Client-Teilnahme in Online-Besprechungen zu unterstützen, werden Verbindungen vom Client Java-Applet zu Sametime erstellt.

Für Besprechungen mit gemeinsam genutzten Anwendungen ist es außerdem nötig, daß ein Besprechungsteilnehmer die Besprechung freigibt. Der Teilnehmer, der die Anwendung freigibt, stellt eine auf seinem lokalen Computer installierte Anwendung anderen Teilnehmern in einer Besprechung mit gemeinsam genutzter Anwendung zur Verfügung. Das Sametime Client Paket umfaßt die OCX-Komponente "Eine Anwendung gemeinsam nutzen". Jeder Client muß diese Komponente installieren, bevor er eine Anwendung gemeinsam nutzt. Die Komponente baut auch eine Verbindung zum Sametime Besprechungsserver auf.

Die Verbindungen von den Java-Applets und der Komponente "Eine Anwendung gemeinsam nutzen" werden durch Anschlüsse auf dem Sametime Server unterstützt. Sametime unterstützt auch Clients, die eine Internet-Verbindung über einen Proxy-Server aufbauen. Weitere Informationen über diese Verbindungen finden Sie unter Verbindung mit dem Besprechungsserver.

Zugriff auf das Besprechungszentrum

Standardmäßig ist anonymer Zugriff auf das Sametime Besprechungszentrum gestattet. Beim anonymen Zugriff muß ein Benutzer keinen Benutzernamen und kein Kennwort eingeben, um die Anwendung zu nutzen. Wenn Benutzer beim Zugriff auf das Besprechungszentrum ein Kennwort eingeben sollen, siehe Deaktivieren des anonymen Zugriffs auf das Sametime Besprechungszentrum.

Verwandte Themen anzeigen
Meeting Services

## Sametime Connect Funktion für gemeinsam genutzte Anwendungen

Der Sametime Connect Client umfaßt die Funktion "Eine Anwendung gemeinsam nutzen". Mit Hilfe dieser Funktion können Benutzer spontane (oder nicht geplante) Besprechungen mit gemeinsam genutzter Anwendung initiieren und andere Benutzer, die gerade online sind, dazu einladen. Ein Benutzer kann Sametime Connect öffnen und mit der rechten Maustaste auf den Namen eines anderen Benutzers, der online ist, klicken, um eine nicht geplante Besprechung mit gemeinsam genutzter Anwendung zu starten. Er kann eine solche Besprechung auch initiieren, während er an einer Konversation teilnimmt, indem er in Sametime Connect "Nachricht - Anwendung gemeinsam nutzen" wählt.

Beim Initiieren einer nicht geplanten Besprechung mit gemeinsam genutzter Anwendung werden folgende Aktionen ausgeführt:

1. Der Initiator der Besprechung lädt einen oder mehrere Benutzer, die gerade online sind, zur Teilnahme an der Besprechung ein.
2. Eine Verbindung zum Besprechungsserver wird aufgebaut und eine Besprechung wird angelegt. Die Verbindung erfolgt über den Anschluß, der in den Verbindungsoptionen des Sametime Connect Clients als Anschluß für gemeinsame Anwendungsnutzung festgelegt ist.
3. Die Komponente "Eine Anwendung gemeinsam nutzen" wird auf dem lokalen Computer des Benutzers gestartet, der die Besprechung initiiert hat. Ein Web-Browser mit dem Client-Java-Applet für die gemeinsame Nutzung wird ebenfalls auf dem Computer dieses Benutzers gestartet. Der Web-Browser baut eine Verbindung zum Sametime HTTP Server auf. Die Komponente "Eine Anwendung gemeinsam nutzen" und das Client-Java-Applet bauen eine Verbindung zu den Meeting Services auf dem Sametime Server auf.
4. Ein entfernter Benutzer erhält eine Besprechungseinladung.
5. Wenn der entfernte Benutzer die Einladung annimmt, wird auf seinem Computer ein Web-Browser gestartet, der das Client-Java-Applet für die gemeinsame Anwendungsnutzung enthält. Der Web-Browser baut eine Verbindung zum Sametime HTTP Server auf. Das Client-Java-Applet baut eine Verbindung zu den Meeting Services auf dem Sametime Server auf.

Die Komponenten "Eine Anwendung gemeinsam nutzen" des Online-Besprechungsraums werden im Web-Browser jedes Benutzers angezeigt und die Benutzer können in einer gemeinsamen Anwendung zusammenarbeiten. Die Benutzer können auch über direkte Nachrichten in Sametime Connect kommunizieren. Die Online-Awareness und Chat-Funktionen von Sametime Connect werden durch die Community Services auf dem Sametime Server unterstützt. Die Online-Besprechungsfunktionen werden durch die Meeting Services unterstützt.

Verwandte Themen anzeigen
Verbindungen von der Komponente "Anwendung gemeinsam nutzen" zum Besprechungsserver

### Meeting Services

Die Komponente "Sametime Besprechungsserver" unterstützt die Meeting Services. Die Meeting Services umfassen die T.120-Software, die Zusammenarbeit in Echtzeit durch gemeinsame Nutzung von Anwendungen sowie eine gemeinsam genutzte Pinwand unterstützt. Die Komponente "Meeting Services" bietet folgende Unterstützung für Online-Besprechungen:

- Sie stellt die Java-Applets für gemeinsame Nutzung von Anwendungen und Pinwand bereit, die alle Clients in der Online-Besprechung verwenden.
- Sie unterstützt eine direkte TCP/IP-, eine SOCKS-Proxy- und eine HTTP-Proxy-Verbindung zwischen den Client Java-Applets und dem Sametime Server. Der Standardanschluß für diese Verbindungen ist Anschluß 8081.
- Sie unterstützt eine direkte TCP/IP-, eine SOCKS-Proxy-, eine HTTPS-Proxy- und eine HTTP-Proxy-Verbindung zwischen dem Client für die gemeinsame Anwendungsnutzung und dem Sametime Server. Der Standardanschluß für diese Verbindungen ist ebenfalls Anschluß 8081.
- Sie unterhält mehrfache Verbindungen und verteilt Daten der Online-Besprechung an alle Teilnehmer der Online-Besprechung.
- Sie unterhält eine Liste der aktiven und geplanten Online-Besprechungen und startet und beendet Besprechungen zur richtigen Zeit.
- Sie trägt Events der Meeting Services im Sametime Protokoll (STLog.nsf) ein.

Sie können die Anschluß-Einstellungen für die Meeting Services auf der Seite "Netzwerk- und Sicherheits-Administration" konfigurieren, die über das Sametime Administrationswerkzeug zur Verfügung stehen. Informationen über andere Administrationseinstellungen der Community Services finden Sie unter Administrationseinstellungen der Meeting Services.

Verwandte Themen anzeigen
Sametime Online-Besprechungszentrum

### Web Application Services

Die Komponente "Web Application Services" von Sametime Server enthält einen HTTP-Web-Server und eine Engine, die Lotus Notes Dateien in HTML konvertiert. Web Application Services unterstützen auch die Internet- und Intranet-Sicherheitsfunktionen von Sametime.

Der HTTP-Web-Server unterstützt Browser-Zugriff auf Sametime. Benutzer mit leistungsfähigen Web-Browsern, wie z. B. Netscape Navigator (v4.06) und Microsoft Internet Explorer (v4.x), können über das Internet oder Intranet eine Verbindung zum Sametime Server herstellen.

Sie können die Einstellungen für die Administration der Services für Web Anwendungen im Serverdokument des Sametime Servers konfigurieren. Sie können die Anschluß-Einstellungen für die Web Application Services auf der Seite "Netzwerk- und Sicherheits-Administration" konfigurieren, die über das Sametime Administrationswerkzeug zur Verfügung stehen.

Verwandte Themen anzeigen
Community Services
Meeting Services

## Domino Application Services

Die Domino Application Services von Sametime unterstützen die Verzeichnis- (Adreßbuch) und die Notes Sicherheits- und Replizierungsfunktionen des Sametime Servers. Die Domino Application Services ermöglichen dem Sametime Server die Zusammenarbeit mit anderen Domino Servern als Teil einer Domino Domäne, wenn Sametime auf einem eigenen Server in einer Domino Umgebung installiert ist.

Wenn Sie Sametime auf einem Server installieren, der bereits Domino enthält, verwendet Sametime den vorhandenen Domino Server für diese Dienste. Wenn Sie Sametime auf einem eigenen Server in einer Domino Domäne installieren, werden die Domino Application Services als Teil von Sametime installiert.

Einige Domino Application Services, z. B. das Verzeichnis, werden auch verwendet, wenn Sametime in einer reinen Web-Umgebung installiert ist. Replizierungs- und Notes-Sicherheitsservices werden in einer reinen Web-Umgebung nicht verwendet.

## Das Sametime Administrationswerkzeug

Das Sametime Administrationswerkzeug wird über einen Web-Browser geöffnet und ist das bevorzugte Administrationswerkzeug für den Sametime Server. Sie können auf das Sametime Administrationswerkzeug von der Seite "Willkommen bei Sametime" (oder der Home Page) aus zugreifen. Das Sametime Administrationswerkzeug können Sie auch öffnen, indem Sie die URL *"http://hostname*/stadmin.nsf" auf Ihrem Web-Browser eingeben (wobei *hostname* der Name oder die IP-Adresse des Sametime Servers ist).

**Hinweis** Das Sametime Administrationswerkzeug ist das bevorzugte Werkzeug für Server-Administration. Wenn Sie Sametime jedoch in einer Domino Umgebung verwenden, können Sie den Server auch verwalten, indem Sie die Serverdokumente der Sametime Server über einen Notes Client öffnen. Viele Sametime Administrationseinstellungen befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Sametime Überwachungsfunktionen stehen auf einem Notes Client nicht zur Verfügung.

Mit dem Sametime Administrationswerkzeug können Sie:

- Sametime Anschlüsse und Netzwerkeinstellungen konfigurieren
- Community Services verwalten
- Meeting Services verwalten
- Meeting Services, Community Services und HTTP-Serveraktivität sowie verfügbaren Plattenplatz überwachen
- Sametime Protokollierungswerkzeuge verwenden
- Benutzer verwalten
- Selbstregistrierung kontrollieren
- Anderen die Benutzung des Sametime Administrationswerkzeugs erlauben
- Zugriff auf den Sametime Server sowie seine Anwendungen und Datenbanken kontrollieren
- Den Secure Sockets Layer einrichten
- Auf Einstellungen für Web Application Services und Domino Application Services im Serverdokument zugreifen

Verwandte Themen anzeigen
Funktionen des Sametime Administrationswerkzeugs

## Sametime Adreßbuch

Das Sametime Adreßbuch ist die zentrale Verzeichnisdatenbank des Sametime Servers. Dieses Verzeichnis enthält Konfigurations- und Sicherheitsinformationen wie Benutzernamen, Kennwörter, Server-Konfigurationseinstellungen, Datenbank-Konfigurationseinstellungen und Listen für die Zugriffskontrolle (ACLs).

Wenn Sie Sametime in einer reinen Web-Umgebung verwenden wollen, enthält das Sametime Adreßbuch drei Dokumente, die Sie für die Administration des Sametime Servers benötigen. Domino Administratoren sollten mit diesen Dokumenten vertraut sein.

| | |
|---|---|
| Person | Enthält Informationen über einen einzelnen Benutzer, wie Benutzername, Internet-Kennwort und Home Sametime Server. |
| Server | Enthält Konfigurationseinstellungen für Komponenten des Sametime Servers. |
| Group | Enthält eine Liste der Benutzer, die die gleichen Aufgaben erfüllen. |

Wenn Sie Sametime in einer Domino Umgebung einsetzen, können Sie das Adreßbuch öffnen, um auf Personen-, Server- und Gruppendokumente zuzugreifen. Diese Dokumente stehen auch über das Sametime Administrationswerkzeug zur Verfügung. Wenn Sie Sametime in einer reinen Web-Umgebung einsetzen, müssen Sie das Sametime Administrationswerkzeug verwenden, um auf diese Dokumente zuzugreifen.

Verwandte Themen anzeigen

Das Personendokument
Das Serverdokument
Das Gruppendokument

## Sametime Adreßbuch in einer Domino Domäne

Wenn Sie Sametime in einer Domino Umgebung installieren, bleibt die Funktion des Buchs im Grunde gleich.

Bei der Installation in einer Domino Umgebung, in der Domino Server mit einer älteren Domino Server Version als 4.6.5 laufen, wird das Adreßbuch auf dem Server geändert, auf dem Sametime läuft. Unabhängig davon, ob Sie Sametime auf einem eigenen Server oder einem Server mit Domino installieren, sollten Sie verhindern, daß das Adreßbuch vom Sametime Server auf den Domino Servern in der Domäne repliziert wird. Installationsanleitungen finden Sie im *Sametime Installationshandbuch*.

Bei der Installation in einer Domino Umgebung, in der Domino Server mit der Domino Server Version 4.6.5 oder höher laufen, werden alle von Sametime verlangten Adreßbuch-Designänderungen in das Domino Release integriert. Die Replizierung des Adreßbuchs von einem Server, auf dem Sametime läuft, auf die Domino Server sollte problemlos verlaufen. Installationsanleitungen finden Sie im *Sametime Installationshandbuch*.

Die Adreßbuch-Designänderungen für einen Sametime Server umfassen einen Abschnitt für den Sametime Server im Serverdokument und ein Feld im Abschnitt "Allgemein" des Serverdokuments, das einen Server als Sametime Server erkennt, sowie ein Feld im Personendokument, das den lokalen Sametime Server eines Benutzers spezifiziert. Im Verlauf der Installation bzw. des Setups geben Sie das Feld für den Home Sametime Server des Benutzers ein. Der Abschnitt "Sametime Server" des Serverdokuments enthält viele Administrationseinstellungen, die auch über das web-basierte Sametime Administrationswerkzeug zur Verfügung stehen.

Der Sametime Connect Client ermöglicht Benutzern, im Adreßbuch eines Sametime Servers zu blättern, um Benutzer und Gruppen zur Connect Liste (oder Teilnehmerliste) hinzuzufügen. Überlappende Adreßbücher und Master Adreßbücher werden unterstützt, wenn Sie mit Hilfe von Sametime Connect Benutzer und Gruppen suchen.

## Das Personendokument

Ein Personendokument enthält Informationen über einen Sametime Benutzer, wie den Namen des Benutzers und dessen Internet-Kennwort. Jedes Mitglied der Sametime Community benötigt ein Personendokument mit Namen und Internet-Kennwort.

Wenn Sie den Sametime Server in einer reinen Web-Umgebung verwenden, erstellen Sie die Personendokumente, sobald Sie Benutzer während der Installation bzw. des Setups hinzufügen. Das Internet-Kennwort wird benötigt, um die Zugriffsberechtigung der Benutzer von Sametime Connect und Sametime Anwendungen auf dem Sametime Server zu prüfen.

Wenn Sie den Sametime Server in einer Domino Umgebung installieren, existieren im Domino Adreßbuch bereits Personendokumente. Jedes Personendokument muß ein Internet-Kennwort enthalten. Das Internet-Kennwort wird benötigt, um die Zugriffsberechtigung der Benutzer von Sametime Connect zu prüfen. Wenn Sie Sametime in einer Domino Umgebung installieren, in der eine ältere Domino Server Version als 4.6.5 läuft, wird das Personendokument im Adreßbuch auf dem Sametime Server während der Installation modifiziert, so daß es ein Sametime Server Feld enthält. Dieses Feld identifiziert den lokalen Sametime Server eines Benutzers. Das Feld ermöglicht, jeden Benutzer einem bestimmten Sametime Server zuzuordnen, wenn mehrere Sametime Server in einer Domino Domäne installiert sind. Das Feld für den lokalen Sametime Server ist ebenfalls erforderlich, wenn Sie Sametime Anwendungen auf einem Server einsetzen. Weitere Informationen hierzu finden Sie unter Verwenden mehrerer Sametime Server.

**Hinweis** Wenn Sie Sametime in einer Domino Umgebung installieren, in der Domino Server Version 4.6.5 oder höher läuft, sollten Personendokumente bereits das Sametime Server Feld enthalten. Die von Sametime verlangten Adreßbuch-Designänderungen sind in Domino Version 4.6.5 oder höher integriert.

Verwandte Themen anzeigen
- Das Serverdokument
- Das Gruppendokument

## Das Serverdokument

Das Serverdokument für den Sametime Server enthält Einstellungen für die Serveradministration.

Wenn Sie den Sametime Server in einer reinen Web-Umgebung installieren, wird das Serverdokument während des Sametime Setups automatisch im Adreßbuch erstellt. Wenn Sie das Sametime Administrationswerkzeug verwenden, ändern Sie Einstellungen im Serverdokument. Sie können das Sametime Administrationswerkzeug auch verwenden, um das Serverdokument zu öffnen und Administrationseinstellungen anzusehen oder zu ändern (dies wird jedoch nicht empfohlen).

Das Serverdokument für den Sametime Server umfaßt einen Abschnitt für Sametime Server, der die Sametime Konfigurationeinstellungen enthält. Sie können mit Hilfe eines Notes Clients oder dem Sametime Administrationswerkzeug auf das Serverdokument auf dem Sametime Server zugreifen. Wählen Sie im Sametime Administrationswerkzeug "Server" und anschließend noch einmal "Server", um auf ein Serverdokument für den Sametime Server zuzugreifen. Sie können das Serverdokument und den Abschnitt für den Sametime Server öffnen, um einige Sametime Konfigurationsoptionen zu sehen.

Lotus empfiehlt die Funktionen des Sametime Administrationswerkzeugs, um Sametime Konfigurationsoptionen zu ändern. Auf alle Konfigurationseinstellungen, die im Abschnitt "Sametime Server" des Serverdokuments zur Verfügung stehen, können Sie bequemer über andere Funktionen des Sametime Administrationswerkzeugs zugreifen. Das Sametime Administrationswerkzeug umfaßt Überwachungsfunktionen, die in anderen Domino Administrationswerkzeugen nicht zur Verfügung stehen.

Zusätzlich wird dem Abschnitt "Allgemein" des Serverdokuments ein Feld "Ist dies ein Sametime Server?" hinzugefügt. Dieses Feld identifiziert den Server für andere Sametime Server als Sametime Server und wird dann benutzt, wenn mehrere Sametime Server in einer Domino Umgebung installiert sind. Weitere Informationen hierzu finden Sie unter Aktivieren mehrerer Sametime Server als einzelne Community.

Verwandte Themen anzeigen
- Das Personendokument
- Das Gruppendokument

### Das Gruppendokument

Gruppendokumente vereinfachen administrative Aufgaben und das Hinzufügen von Benutzern zum Sametime Connect Client.

Ein Gruppendokument enthält eine Liste von Benutzern, die dieselbe Aufgabe ausführen. Mit Hilfe von Gruppendokumenten können Sie häufig wiederkehrende Aufgaben für Administratoren und Sametime Connect Benutzer reduzieren. Wenn beispielsweise in einer fiktiven Marketingabteilung 40 Angestellte arbeiten, kann der Administrator ein Dokument für die Marketing-Gruppe erstellen, das die Namen der 40 Angestellten dieser Abteilung enthält. Jeder Angestellte der Marketingabteilung kann die Marketing-Gruppe auf die Connect Liste in Sametime Connect setzen und dadurch sofort Online-Awareness und Chat-Funktionen mit allen Mitgliedern der Marketingabteilung ausführen. Ohne das Gruppendokument müßte der Benutzer alle 40 Namen einzeln eingeben. Gruppendokumente vermindern außerdem Wiederholungen für die Administration, wenn sie Namen zu Listen für die Zugriffskontrollisten (ACLs) für Sametime Anwendungen und Datenbanken hinzufügen.

Verwandte Themen anzeigen
- Das Personendokument
- Das Serverdokument

### Sametime Sicherheit

Der Sametime Server hat dieselben Internet- und Intranet-Sicherheitsfunktionen, wie sie auf einem Domino Server erhältlich sind. Wenn Sie den Sametime Server als reinen Web-Server verwenden und mit den Domino Internet- und Intranet-Sicherheitsfunktionen nicht vertraut sind, sollten Sie alle Themen über Sicherheit wiederholen, bevor Sie die Standardeinstellungen des Sametime Servers ändern.

Zusätzlich zu den Domino Internet- und Intranet-Sicherheitsfunktionen richtet der Sametime Server Sicherheitsrichtlinien ein, um die Berechtigung der Sametime Benutzer für Verbindungen zu Meeting Services und Community Services zu überprüfen. Diese Sicherheitsrichtlinien werden unter Authentifizierung von Verbindungen zum Sametime Server kurz beschrieben.

Secure Sockets Layer (SSL) 3.0, ein leistungsfähiges Sicherheitsprotokoll, wird vom Sametime Server für Firmen unterstützt, die strenge Sicherheitsvorkehrungen benötigen.

**Hinweis** Der Abschnitt "Sicherheit" des Sametime Administrationshandbuchs erläutert Internet- und Intranet-Sicherheitsfunktionen. Hinweise zur Sicherheit für Notes Benutzer finden Sie in Ihrer Domino Administrationsdokumentation.

# Kapitel 02: Verwenden des Sametime Administrationswerkzeugs

## Funktionen des Sametime Administrationswerkzeugs

Mit dem Sametime Administrationswerkzeug können Sie Ihren Sametime Server über einen Browser verwalten. Starten Sie das Sametime Administrationswerkzeug, indem Sie "Server-Administration" auf der Seite "Willkommen bei Sametime" wählen.

**Hinweis** Wenn Sie Sametime in einer Domino Umgebung installieren, können Sie auch den Server verwalten, indem Sie die Serverdokumente der Sametime Server über einen Notes Client öffnen. Viele Sametime Administrationseinstellungen befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Jedoch ist das Sametime Administrationswerkzeug das bevorzugte administrative Werkzeug. Es umfaßt Sametime Überwachungsfunktionen, die in anderen Domino Administrationswerkzeugen nicht zur Verfügung stehen.

Mit dem Sametime Administrationswerkzeug können Sie:

- Sametime Anschlüsse und Netzwerkeinstellungen konfigurieren
- Community Services verwalten
- Meeting Services verwalten
- Benutzer verwalten
- Nachrichten an Online-Benutzer senden
- Den Sametime Server überwachen
- Sametime Protokolle verwenden und einrichten
- Auf Einstellungen für Web Application Services und Domino Application Services im Serverdokument zugreifen
- Sicherheit verwalten.
- Den Secure Sockets Layer einrichten
- Anderen Benutzern Zugriffsrechte auf das Sametime Administrationswerkzeug einräumen
- Zur Seite "Willkommen bei Sametime" zurückblättern
- Auf die Online-Hilfe für das Sametime Administrationswerkzeug zugreifen.

Weitere Informationen über die einzelnen Befehle finden Sie unter Überblick über Befehle des Sametime Administrationswerkzeugs.

Verwandte Themen anzeigen

Starten des Sametime Administrationswerkzeugs

## Starten des Sametime Administrationswerkzeugs

Das Sametime Administrationswerkzeug können Sie über die Seite "Willkommen bei Sametime" starten, oder indem Sie eine URL in Ihrem Web-Browser eingeben.

**Hinweis** Sie müssen Java-Applets und JavaScript oder ActiveX Script in Ihrem Browser aktivieren, um das Sametime Administrationswerkzeug zu verwenden.

**Starten des Sametime Administrationswerkzeugs durch Eingabe einer URL**
Sie können das Sametime Administrationswerkzeug starten, indem Sie die folgende URL eingeben:

`http://`*`hostname`*`/stadmin.nsf`

Hierbei ist *hostname* der Name des Hosts oder die IP-Adresse des Sametime Servers, den Sie verwalten wollen.

Nach Eingabe der URL geben Sie den Administratornamen und das Kennwort ein, das während des Sametime Setup-Programms festgelegt wurde.

**Starten des Sametime Administrationswerkzeugs auf der Seite "Willkommen bei Sametime"**
Von der Seite "Willkommen bei Sametime" aus starten Sie das Sametime Administrationswerkzeug wie folgt:

1. Starten Sie Ihren Browser.
2. Aktivieren Sie falls nötig Java-Applets und JavaScript oder ActiveX Script in Ihrem Browser. Weitere Informationen hierzu finden Sie in der Dokumentation Ihres Browsers.
3. Geben Sie die URL für den Sametime Server ein:

   `http://`*`hostname`*

   Hierbei ist *hostname* der Name des Hosts oder die IP-Adresse des Sametime Servers, den Sie verwalten wollen.
4. Klicken Sie auf der Seite "Willkommen bei Sametime" auf "Server-Administration".
5. Geben Sie den Administratornamen und das Kennwort ein, das im Sametime Setup-Programm festgelegt wurde.

Wie Sie anderen Benutzern Zugriff auf das Sametime Administrationswerkzeug ermöglichen, erfahren Sie unter Anderen Benutzern Zugriffsrechte auf das Sametime Administrationswerkzeug einräumen.

**Hinweis** Nach Zugriff auf das Sametime Administrationswerkzeug können Sie zur Seite "Willkommen bei Sametime" zurückkehren, indem Sie auf das Lotus Sametime Logo in der unteren linken Ecke des Sametime Administrationswerkzeugs klicken.

Verwandte Themen anzeigen
- Details: Starten des Sametime Administrationswerkzeugs
- Starten des Sametime Administrationswerkzeugs durch Eingabe einer URL
- Starten des Sametime Administrationswerkzeugs auf der Seite "Willkommen bei Sametime"

## Details: Starten des Sametime Administrationswerkzeugs

Um das Sametime Administrationswerkzeug in Internet Explorer 4.x auszuführen, treffen Sie im Internet Explorer die folgenden Einstellungen. Diese Einstellungen sind unabhängig davon erforderlich, ob Internet Explorer auf einem Client- oder Server-Computer installiert ist.

1. Wählen Sie "Ansicht - Internet-Optionen".
2. Wählen Sie das Register "Erweitert".
3. Entfernen Sie die Markierung von der Option "HTTP 1.1 verwenden".

Stellen Sie die Standardschrift in Ihrem Browser auf eine kleine Schriftgröße ein, um sicherzustellen, daß alle Befehlsgruppen und Befehle im verfügbaren Platz im Sametime Administrationswerkzeug sichtbar sind.

Um gleichzeitig mehrere Versionen des Sametime Administrationswerkzeugs zu sehen (z. B. zur Überwachung von Verbindungen zu Community Services und Meeting Services), starten Sie weitere Kopien des Browsers und öffnen Sie das Sametime Administrationswerkzeug in jeder Browser-Kopie. Ordnen Sie die Fenster so an, daß alle Kopien am Bildschirm sichtbar sind.

Für den Zugriff auf das Sametime Administrationswerkzeug müssen Sie den Benutzernamen eingeben, der während der Sametime Installation für den Administrator angegeben wurde. Wie Sie anderen Benutzern den Zugriff auf das Sametime Administrationswerkzeug ermöglichen, erfahren Sie unter Anderen Benutzern Zugriffsrechte auf das Sametime Administrationswerkzeug einräumen.

Verwandte Themen anzeigen
Starten des Sametime Administrationswerkzeugs

## Überblick über Befehle des Sametime Administrationswerkzeugs

Das Sametime Administrationswerkzeug umfaßt fünf Befehlsgruppen: Server, Überwachung, Protokolle, Benutzer und Hilfe.

Führen Sie administrative Funktionen aus, indem Sie eine der Befehlsgruppen und dann einen Befehl aus der Liste dieser Befehlsgruppe wählen. So können Sie zum Beispiel einen neuen Benutzer hinzufügen, indem Sie die Befehlsgruppe "Benutzer" und dann den Befehl "Teilnehmer hinzufügen" wählen.

### Befehlsgruppe "Server"

Nachstehende Tabelle beschreibt die Befehlsgruppe "Server" des Sametime Administrationswerkzeugs:

| **Server** | **Beschreibung** |
|---|---|
| Netzwerk und Sicherheit | Für das Konfigurieren der Sametime Anschlüsse und Unterstützen von Clients, die über einen Proxy-Computer oder HTTP-Proxy-Tunneling mit dem Server verbunden werden. Weitere Informationen finden Sie unter Sametime Anschlüsse und Netzwerkeinstellungen.<br>Ermöglicht auch das Ein- und Ausschalten der Selbstregistrierung. Die Funktion der Selbstregistrierung ist verfügbar, wenn Sametime als reiner Web-Server eingesetzt wird. Weitere Informationen finden Sie unter Verwenden der Selbstregistrierung. |
| Community Services | Für das Konfigurieren von Community Services zur Unterstützung mehrerer Sametime Server. Sie können auch festlegen, wie Community Services mit dem Adreßbuch interagieren. Weitere Informationen finden Sie unter Administrationseinstellungen für Community Services. |
| Meeting Services | Für das Verlängern von Besprechungen über die festgelegte Endzeit hinaus, das Auflisten von Besprechungsteilnehmern auf Besprechungsdokumenten und Erstellen der erforderlichen Verbindungsdokumente, damit mehrere Sametime Server als Host für dieselbe Besprechung fungieren können. Weitere Informationen finden Sie unter Administrationseinstellungen für Meeting Services. |

| | |
|---|---|
| Server | Gestattet den Zugriff auf das Serverdokument. Das Serverdokument enthält Administrationseinstellungen, die HTTP-Server, Sicherheit und Domino Application Services beeinflussen. Weitere Informationen finden Sie unter Administrationseinstellungen für das Serverdokument. |
| Nachricht senden | Für das Senden einer Nachricht an alle Benutzer, die gerade über Sametime Connect oder eine Sametime Anwendung bei den Community Services angemeldet sind. Weitere Informationen finden Sie unter Senden von Nachrichten. |
| Datenbanksicherheit | Für die Verwaltung von Anwendungs- und Datenbank-Zugriffskontrollisten (ACLs). Weitere Informationen finden Sie unter Datenbank-Zugriffskontrollisten (ACLs). |

### Befehlsgruppe "Überwachung"

Nachstehende Tabelle beschreibt die Befehlsgruppe "Überwachung" des Sametime Administrationswerkzeugs:

| Überwachung | Beschreibung |
|---|---|
| Community Server | Zeigt grafische Darstellungen der Gesamtanzahl an Benutzern, die bei Community Services angemeldet sind, sowie die Anzahl eindeutiger Anmeldungen bei Community Services. Weitere Informationen finden Sie unter Überwachung des Community Servers . |
| Besprechungsserver | Zeigt grafische Darstellungen der Anzahl an aktiven Online-Besprechungen, der Anzahl der Teilnehmer pro Besprechung und die Anzahl fehlgeschlagener Authentifizierungen pro Besprechung. Weitere Informationen finden Sie unter Überwachung des Besprechungsservers. |
| HTTP | Zeigt grafische Darstellungen von Umfang und Art der HTTP-Anforderungen und -Befehle, die der Server verarbeitet. Weitere Informationen finden Sie unter Überwachung der HTTP-Statistik. |
| Speicherplatz | Zeigt eine grafische Darstellung des verfügbaren Speicherplatzes auf dem Sametime Server. Weitere Informationen finden Sie unter Überwachung des Speicherplatzes. |

### Befehlsgruppe "Protokolle"

Nachstehende Tabelle beschreibt die Befehlsgruppe "Protokolle" des Sametime Administrationswerkzeugs:

| Protokolle | Beschreibung |
|---|---|
| Sametime Protokoll | Für den Zugriff auf das Protokoll, das Ereignisse von Meeting Services und Community Services aufzeichnet. Weitere Informationen finden Sie unter Sametime Protokoll. |
| Notes Protokoll | Weitere Informationen über das Notes Protokoll finden Sie unter Notes Protokolldatenbank. |
| Protokollparameter | Für die Angabe von Dateityp und Speicherort des Sametime Protokolls sowie der Arten von Community Services und Meeting Services Ereignissen, die protokolliert werden sollen. Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll. |

### Befehlsgruppe "Benutzer"

Nachstehende Tabelle beschreibt die Befehlsgruppe "Benutzer" des Sametime Administrationswerkzeugs:

| Benutzer | Beschreibung |
|---|---|
| Teilnehmer hinzufügen | Für die rasche Aufnahme von Teilnehmern in das Sametime Adreßbuch. Weitere Informationen finden Sie unter Hinzufügen eines neuen Benutzers. |
| Teilnehmer | Für den Zugriff auf das Personendokument eines Benutzers im Sametime Adreßbuch. Sie können das Personendokument bearbeiten oder den Benutzer aus dem Adreßbuch löschen. Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines bestehenden Benutzers. |
| Gruppen | Für das Hinzufügen, Bearbeiten oder Löschen von Gruppendokumenten im Sametime Adreßbuch. Weitere Informationen finden Sie unter Verwenden von Gruppendokumenten. |

### Befehlsgruppe "Hilfe"

Nachstehende Tabelle beschreibt die Befehlsgruppe "Hilfe" des Sametime Administrationswerkzeugs:

| Hilfe | Beschreibung |
|---|---|
| Hilfethemen | Bietet Sametime Administratoren Zugriff auf die Online-Hilfe. |
| Info über Sametime | Bietet Sametime Administratoren Zugriff auf die Online-Hilfe. |

Verwandte Themen anzeigen

Starten des Sametime Administrationswerkzeugs

## Einräumen von Zugriffsrechten auf das Sametime Administrationswerkzeug für andere Benutzer

Um weiteren Personen Zugriffsrechte auf das Sametime Administrationswerkzeug einzuräumen, gehen Sie wie folgt vor:

1. Ändern Sie die ACL des Sametime Administrationswerkzeugs (STADMIN.NSF). Sie müssen den Benutzernamen des neuen Administrators in die Zugriffskontrolliste (ACL) einfügen und die gewünschten Funktionen für den Administrator zuweisen.
2. Ändern Sie die ACL des Sametime Adreßbuchs. Sie müssen den Benutzernamen des neuen Administrators in die ACL des Adreßbuchs einfügen, dem Benutzernamen die Zugriffsebene "Verwalter" zuweisen und die gewünschten Funktionen für den Administrator festlegen.
3. Ändern Sie das Serverdokument des Sametime Servers. Sie müssen den Benutzernamen des Administrators in die Felder "Server von einem Browser aus verwalten" und "Unbeschränkte LotusScript/Java-Agenten ausführen" im Serverdokument des Sametime Servers eingeben.

Wenn Sie beabsichtigen, für viele Benutzer Zugriff zum Sametime Administrationswerkzeug einzurichten, sollten Sie zunächst eine Administratorengruppe erstellen. Das Erstellen von Gruppen ermöglicht Ihnen, mehrere Benutzer, die dieselbe Aufgabe wahrnehmen, effizient zu verwalten. Weitere Informationen hierzu finden Sie unter Info über das Erstellen von Gruppendokumenten.

Verwandte Themen anzeigen

Ändern der ACL des Sametime Administrationswerkzeugs
Ändern des Serverdokuments des Sametime Servers
Ändern der ACL des Sametime Adreßbuchs

## Ändern der ACL des Sametime Administrationswerkzeugs

Dieser Vorgang ist der erste von drei Schritten, die nötig sind, um anderen Benutzern Zugriffsrechte auf das Sametime Administrationswerkzeug einzuräumen.

Bei dieser Prozedur fügen Sie der ACL der Sametime Administrationswerkzeug-Datenbank (STAdmin.nsf) Benutzer- oder Gruppennamen hinzu und weisen die Zugriffsebene "Verwalter" zu. Sie müssen auch die geeigneten Funktionen für jeden Benutzer- oder Gruppennamen festlegen.

**Hinweis** Wenn Sie mehreren Benutzern Zugriff gewähren und Sie eine Administratorengruppe erstellt haben, können Sie diesen Prozeß einmal ausführen. Wenn Sie mehrere Benutzer einzeln hinzufügen, müssen Sie diese Schritte für jeden Benutzer wiederholen.

Benutzer dem Sametime Administrationswerkzeug als Verwalter hinzufügen:

1. Klicken Sie auf der Seite "Willkommen bei Sametime" auf "Server Administration".
2. Geben Sie den Administratornamen und das Kennwort ein.
3. Wählen Sie "Server" und danach "Datenbanksicherheit".
4. Wählen Sie aus der Datenbankliste "Sametime Web Admin".
5. Klicken Sie auf die Schaltfläche "Zugriff".
6. Klicken Sie auf die Schaltfläche "Hinzufügen". Geben Sie den Namen des Benutzers im Dialogfeld ein. (Geben Sie den Namen genau so ein, wie er im Feld "Benutzername" des Personendokuments eingegeben wurde.)

   Geben Sie den Gruppennamen anstelle des Personennamens ein, wenn Sie für die Administratoren ein Gruppendokument erstellt haben.
7. Klicken Sie auf OK.
8. Wählen Sie den Namen der Person aus der Liste im Fenster "Datenbanksicherheit".
9. Wählen Sie "Teilnehmer" in der Auswahlliste "Benutzertyp" (oder "Gruppe", wenn Sie für die Administratoren ein Gruppendokument erstellt haben).
10. Wählen Sie in der Zugriffsliste "Verwalter".

    **Hinweis** Stellen Sie sicher, daß das Auswahlfeld "Dokumente löschen" der Zugangsliste ausgewählt ist.
11. Klicken Sie auf die Schaltfläche "Funktionen".
12. Wenn der Administrator die gesamte Palette von administrativen Funktionen erhalten soll, wählen Sie alle drei Funktionen aus: ServerAdmin, ServerMonitor und DatabaseAdmin. Eine Funktion ist dann ausgewählt, wenn sie markiert ist. Klicken Sie auf OK.

    Die Funktionen, die Sie einem Administrator zuweisen, legen fest, welche administrativen Aufgaben er durchführen kann. Weitere Informationen über administrative Funktionen finden Sie unter Info über Sametime Administrationsfunktionen.
13. Klicken Sie auf "Senden". Wiederholen Sie Schritt 6 bis 13 für jede Person (oder Gruppe), die auf das Sametime Administrationswerkzeug zugriffsberechtigt sein soll.
14. Nachdem Sie die ACL des Sametime Administrationswerkzeugs geändert haben, müssen Sie die ACL des Sametime Adreßbuchs ändern.

Verwandte Themen anzeigen

Ändern des Serverdokuments des Sametime Servers
Ändern der ACL des Sametime Adreßbuchs
Funktionen des Sametime Administrationswerkzeugs
Funktionen im öffentlichen Adreßbuch

## Ändern der ACL des Sametime Adreßbuchs

Diese Vorgehensweise ist der zweite von drei erforderlichen Schritten, um Benutzern Zugriff auf das Sametime Administrationswerkzeug einzuräumen. Die Personen-, Server- und Gruppendokumente, die die Sametime Administrationseinstellungen enthalten, befinden sich in einer Datenbank, die "Adreßbuch" heißt.  Wenn Sie das Sametime Administrationswerkzeug verwenden, um Einstellungen zu ändern, greifen Sie auf ein Dokument im Adreßbuch zu. Deshalb muß einem Administrator ein Zugriffsrecht in der Adreßbuch-ACL zugewiesen werden.

1. Wählen Sie "Server" und dann "Datenbanksicherheit" im Sametime Administrationswerkzeug. (Dieses Fenster ist bereits geöffnet, wenn Sie gerade die ACL des Sametime Administrationswerkzeugs geändert haben.)
2. Wählen Sie "Adreßbuch" aus der Datenbankliste. (Der Name der Adreßbuch-Datenbank enthält normalerweise den Community-Namen, wie z. B. "Acme Adreßbuch". Der Dateiname des Adreßbuchs lautet NAMES.NSF.)
3. Klicken Sie auf die Schaltfläche "Zugriff".
4. Klicken Sie auf die Schaltfläche "Hinzufügen". Geben Sie den Benutzernamen der Person (oder einen Gruppennamen) in das Dialogfeld ein.
5. Klicken Sie auf OK.
6. Wählen Sie den Namen der Person (oder Gruppe) aus der Liste im Fenster "Datenbanksicherheit".
7. Wählen Sie "Person" (oder "Gruppe") aus der Benutzertyp-Liste.
8. Wählen Sie "Verwalter" aus der Zugriffsliste.
9. Stellen Sie sicher, daß das Auswahlfeld  "Dokumente löschen" der Zugriffsliste ausgewählt ist.
10. Klicken Sie auf "Funktionen".
11. Wenn der Administrator über Zugriff auf alle Administrationseinstellungen verfügen soll, wählen Sie alle Funktionen aus. Klicken Sie auf OK.

    Die Funktionen, die einem Administrator im öffentlichen Adreßbuch zugewiesen werden, bestimmen, welche Dokumente er bearbeiten kann. Weitere Informationen über die Administrationsfunktionen finden Sie unter Info über Funktionen im öffentlichen Adreßbuch.
12. Klicken Sie auf "Senden". Wiederholen Sie Schritt 4 bis 12 für alle Personen, die das Sametime Administrationswerkzeug verwenden sollen.
13. Nachdem Sie die ACL des Sametime Adreßbuchs geändert haben, müssen Sie das Serverdokument des Sametime Servers ändern.

    Verwandte Themen anzeigen
    - Ändern der ACL des Sametime Administrationswerkzeugs
    - Ändern des Serverdokuments des Sametime Servers
    - Funktionen des Sametime Administrationswerkzeugs
    - Funktionen im öffentlichen Adreßbuch

## Ändern des Serverdokuments des Sametime Servers

Dieser Vorgang ist der letzte von drei Schritten, die nötig sind, um anderen Benutzern Zugriffsrechte auf das Sametime Administrationswerkzeug einzuräumen. Sie können anderen Benutzern (oder Gruppen) Zugriffsrechte auf das Sametime Administrationswerkzeug einräumen, indem Sie deren Namen in zwei Felder des Serverdokuments eintragen: das Feld "Server von einem Browser aus verwalten" im Abschnitt "Beschränkungen" und das Feld "Unbeschränkte LotusScrip-Agenten ausführen" im Abschnitt "Agent-Manager". Sie tragen Benutzer folgendermaßen in diese Felder ein:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und danach erneut "Server". Eine Liste verfügbarer Serverdokumente erscheint im Fensterbereich rechts.
2. Klicken Sie auf den Namen des Sametime Servers, um das Serverdokument zu öffnen.
3. Klicken Sie auf "Server bearbeiten".

4. Blättern Sie zum Abschnitt "Beschränkungen". Geben Sie im Feld "Server von einem Browser aus verwalten" jeweils den Namen eines Benutzers ein (oder einer Gruppe, wenn Sie eine Administratorengruppe erstellt haben).

   **Hinweis** Geben Sie den Benutzernamen genau so ein, wie er im Feld "Benutzername" des Personendokuments eingegeben wurde. Geben Sie einen Gruppennamen genau so ein, wie er im Gruppendokument eingegeben wurde. Trennen Sie unbedingt mehrere Namen jeweils durch ein Komma.

5. Blättern Sie zum Abschnitt "Agent-Manager". Geben Sie im Feld "Unbeschränkte LotusScript/Java-Agenten ausführen" den Benutzer- oder Gruppennamen ein. Falls dieses Feld bereits Einträge enthält, geben Sie ein Komma hinter dem letzten Eintrag ein und danach den Benutzer oder Gruppennamen.
6. Speichern Sie das Serverdokument, indem Sie am oberen Rand des Dokuments auf "Speichern und Schl ießen" klicken.

Verwandte Themen anzeigen

Ändern der ACL des Sametime Administrationswerkzeugs
Ändern der ACL des Sametime Adreßbuchs
Funktionen des Sametime Administrationswerkzeugs
Funktionen im öffentlichen Adreßbuch

## Funktionen des Sametime Administrationswerkzeugs

Das Sametime Administrationswerkzeug verwendet drei Funktionen, um den Benutzern zur Verfügung stehende Befehle zu kontrollieren. Wenn Sie anderen Benutzern Zugriff auf das Sametime Administrationswerkzeug einräumen, müssen Sie jedem Benutzer eine Funktion zuweisen. Die drei Funktionen sind "ServerMonitor", "ServerAdmin" oder "DatabaseAdmin".

Funktionen ermöglichen es, den Zugriff des Administrators auf die Sametime Server Einstellungen zu konkretisieren. Wenn Sie beispielsweise einem Administrator nur die Funktion "ServerMonitor" zuweisen, kann der Administrator Serverspeicher, Festplattenspeicher und andere Serverstatistik überwachen, aber keine anderen administrativen Funktionen ausführen. Wenn der Administrator Zugriff auf alle Befehle des Sametime Administrationswerkzeugs haben soll, weisen Sie ihm alle drei Funktionen zu.

Folgende Tabelle enthält die Befehle des Sametime Administrationswerkzeugs und die erforderliche Funktion, die ein Administrator haben muß, um Sie zu benutzen. Wenn Sie nicht über die entsprechende Funktion verfügen, zeigt das Sametime Administrationswerkzeug den Befehl nicht an.

| Befehlsgruppe | Befehl | Erforderliche Funktion |
|---|---|---|
| Server | Netzwerk und Sicherheit, Community Services, Meeting Services, Server, Nachrichten senden | [ServerAdmin] oder [ServerMonitor] Ein Benutzer mit der Funktion "ServerMonitor" kann Einstellungen für diese Befehle ansehen, aber nicht ändern. |
| Server | Datenbanksicherheit | [DatabaseAdmin] oder [ServerAdmin] |
| Überwachung | Community Server, Besprechungsserver, HTTP Statistik, Speicherplatz | [ServerMonitor] oder [ServerAdmin] |
| Protokolle | Sametime Protokoll, Notes Protokoll, Protokollparameter | [ServerMonitor] oder [ServerAdmin] |
| Benutzer | Benutzer hinzufügen, Teilnehmer, Gruppen | [ServerAdmin] oder [DatabaseAdmin] |
| Hilfe | | Keine Funktion erforderlich |

Verwandte Themen anzeigen
Funktionen im öffentlichen Adreßbuch

## Funktionen im öffentlichen Adreßbuch

Das öffentliche Adreßbuch enthält Benutzer-, Personen- und Gruppendokumente, die Sie erstellen und bearbeiten, wenn Sie das Sametime Administrationswerkzeug verwenden. Die Funktionen im öffentlichen Adreßbuch legen fest, wer eine bestimmte Dokumentenart erstellen oder bearbeiten kann.

Wenn Sie Sametime in einer Domino Umgebung verwenden, entsprechen die Funktionen des öffentlichen Adreßbuchs denen auf einem Domino Server. Wenn Sie den Sametime Server als reinen Web-Server einsetzen, können Sie gewöhnlich jedem Administrator alle Funktionen zuweisen.

Das öffentliche Adreßbuch enthält acht Funktionen. Die Privilegien für jede Funktion werden in der folgenden Tabelle aufgeführt:

| Funktion | Beschreibung |
|---|---|
| UserCreator | Ermöglicht dem Administrator, Personendokumente im Sametime Adreßbuch zu erstellen |
| UserModifier | Ermöglicht dem Administrator, alle Personendokumente im Sametime Adreßbuch zu bearbeiten |

| | |
|---|---|
| GroupCreator | Ermöglicht dem Administrator, Gruppendokumente im Sametime Adreßbuch zu erstellen |
| GroupModifier | Ermöglicht dem Administrator, alle Gruppendokumente im Sametime Adreßbuch zu bearbeiten |
| ServerCreator | Ermöglicht dem Administrator, Serverdokumente im Sametime Adreßbuch zu erstellen |
| ServerModifier | Ermöglicht dem Administrator, alle Serverdokumente im Sametime Adreßbuch zu bearbeiten |
| NetCreator | Wird nicht verwendet, wenn Sametime als reiner Web-Server eingesetzt wird |
| NetModifier | Wird nicht verwendet, wenn Sametime als reiner Web-Server eingesetzt wird |

Verwandte Themen anzeigen
Funktionen des Sametime Administrationswerkzeugs

### Zurückblättern zur Seite "Willkommen bei Sametime"

Wenn Sie das Sametime Administrationswerkzeug geöffnet haben, können Sie zur Seite "Willkommen bei Sametime" zurückkehren, indem Sie auf das Lotus Sametime Logo in der linken unteren Ecke des Sametime Administrationswerkzeugs klicken.

Sie können auch den Browser schließen, um das Sametime Administrationswerkzeug zu beenden.

# Kapitel 03: Verwalten von Benutzern

## Verwalten von Sametime Benutzern

Die Sametime Community besteht aus allen Benutzern, die über ein Personendokument im Sametime Adreßbuch verfügen. Das Personendokument enthält Informationen über den Sametime Benutzer, einschließlich seines Benutzernamens und Internet-Kennworts. Das Personendokument muß einen Benutzernamen und ein Internet-Kennwort für den Benutzer enthalten, damit dieser auf den Sametime Connect Client oder auf geschützte Bereiche des Sametime Servers mit einem Web-Browser zugreifen kann.

Wenn Sie mit Hilfe des Sametime Administrationswerkzeugs einen Benutzer hinzufügen, wird für den Benutzer automatisch ein Personendokument (einschließlich Benutzername und Internet-Kennwort) im Sametime Adreßbuch angelegt. Wenn Sie Informationen für einen Benutzer ändern wollen, wie z. B. das Internet-Kennwort, müssen Sie das Personendokument des Benutzers bearbeiten. Um einen Benutzer aus der Sametime Community zu entfernen, müssen Sie das Personendokument des Benutzers aus dem Adreßbuch löschen.

Falls Sie Sametime in einer Domino Umgebung einsetzen und die Benutzer über Lotus Notes Clients auf den Sametime Server zugreifen, siehe Verwalten von Benutzern in einer Notes/Domino Umgebung.

Mit Hilfe von Gruppendokumenten können Sie Benutzer in Gruppen organisieren, um administrative Prozeduren zu vereinfachen und sich wiederholende Aufgaben zu verringern. Gruppendokumente erleichtern es auch Endbenutzern, Personen in die Sametime Connect Client Verbindungsliste aufzunehmen.

Zu den grundlegenden Sicherheitsthemen rund um die Benutzerverwaltung gehören die Selbstregistrierung und das Anfordern eines Kennworts für den Zugriff auf das Online-Besprechungszentrum. Diese Themen werden im Abschnitt "Erläuterung von Sicherheit" der vorliegenden Dokumentation behandelt.

Verwandte Themen anzeigen
- Details: Verwalten von Sametime Benutzern
- Hinzufügen eines neuen Benutzers
- Bearbeiten oder Löschen eines bestehenden Benutzers
- Erstellen einer Gruppe
- Bearbeiten oder Löschen einer Gruppe

## Details: Verwalten von Sametime Benutzern

Wenn Benutzer mit Lotus Notes Clients auf das Online-Besprechungszentrum zugreifen sollen, siehe Verwalten von Benutzern in einer Notes/Domino Umgebung.

Das Sametime Online-Besprechungszentrum (STCONF.NSF) gestattet standardmäßig anonymen Zugriff. Jeder anonyme Benutzer kann auf das Online-Besprechungszentrum zugreifen und neue Online-Besprechungen anlegen, ohne durch den Server authentifiziert zu werden. Schalten Sie anonymen Zugriff aus, indem Sie die Zugriffskontrolliste (ACL) des Online-Besprechungszentrums (STCONF.NSF) ändern. Wenn anonymer Zugriff ausgeschaltet ist, muß ein Web-Browser-Benutzer den Benutzernamen und das Internet-Kennwort aus seinem Personendokument eingeben, um Zugriff auf das Online-Besprechungszentrum zu erhalten. Weitere Informationen finden Sie unter Ausschalten des anonymen Zugriffs auf das Sametime Besprechungszentrum. Lotus Notes Benutzer werden durch den Domino Authentifizierungsprozeß identifiziert.

Der Sametime Server umfaßt eine Funktion zur Selbstregistrierung. Diese Funktion wird nur unterstützt, wenn Sametime in einer Domino Umgebung installiert ist. Durch Selbstregistrierung kann jeder anonyme Benutzer, der auf den Server zugreifen kann, sein eigenes Personendokument mit Benutzernamen und Internet-Kennwort anlegen. Diese Benutzer können den Sametime Connect Client herunterladen und verwenden und auf alle geschützten Bereiche des Sametime Servers, mit Ausnahme des Sametime Administrationswerkzeugs, zugreifen. Die Selbstregistrierung können Sie ein- und ausschalten. Standardmäßig ist Selbstregistrierung ausgeschaltet, da sie für einige Unternehmen ein Sicherheitsrisiko darstellt. Siehe Verwenden der Selbstregistrierung, bevor Sie entscheiden, ob Sie Selbstregistrierung gestatten wollen.

## Hinzufügen eines neuen Benutzers

Diese Prozedur legt automatisch im Sametime Adreßbuch ein Personendokument mit einem Internet-Kennwort für einen Benutzer an.

So fügen Sie einen neuen Benutzer hinzu:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Administratorname und -kennwort ein, um das Sametime Administrationswerkzeug zu öffnen.
3. Wählen Sie "Benutzer" und dann "Teilnehmer hinzufügen".
4. Geben Sie Vornamen und Name des Benutzers in die entsprechenden Felder ein. Der Nachname ist obligatorisch, erster und zweiter Vorname sind optional.

   Bei der Eingabe dieser Daten wird das Feld "Benutzername" automatisch ausgefüllt. Der Benutzername umfaßt auch den Community-Namen.

   **Hinweis** Wenn ein Benutzer zur Eingabe seines Benutzernamens aufgefordert wird, kann er den Namen wie in den Feldern für Vornamen und Nachnamen schreiben. Er kann bei der Anmeldung aber auch den vollständigen Benutzernamen (samt Community-Namen) eingeben.
5. Geben Sie ein Internet-Kennwort für die Person in das Feld "Internet-Kennwort" ein. Der Benutzer wird bei der Anmeldung zu Sametime Connect oder beim Zugriff auf geschützte Bereiche des Sametime Servers mit einem Web-Browser zur Eingabe dieses Kennworts augefordert. Bezüglich der verwendeten Zeichenanzahl gibt es für das Internet-Kennwort keine Beschränkung.

   Schreiben Sie die Internet-Kennwörter auf, wie Sie sie zuweisen. Das Internet-Kennwort wird im Personendokument verschlüsselt und kann nicht angezeigt werden.
6. Klicken Sie auf "Hinzufügen".
7. Das Feld "Statusmeldungen" zeigt an, ob der Benutzer erfolgreich hinzugefügt wurde.

Sie können über das Sametime Administrationswerkzeug auf das Personendokument jedes Benutzers zugreifen, indem Sie "Benutzer" und dann "Teilnehmer" wählen. Das Internet-Kennwort für jeden Benutzer ist im Personendokument verschlüsselt.

Verwandte Themen anzeigen
Details: Hinzufügen eines neuen Benutzers

## Details: Hinzufügen eines neuen Benutzers

Um auf Sametime Connect oder einen geschützten Bereich des Sametime Servers mit einem Web-Browser zuzugreifen, muß der Benutzer seinen Benutzernamen und sein Internet-Kennwort eingeben. Wenn Sie einen Benutzer mit dem Sametime Administrationswerkzeug hinzugefügt haben, enthält das Feld "Benutzername" des Personendokuments die Namen, die ein Benutzer eingeben kann, wenn er zur Eingabe des Benutzernamens aufgefordert wird. In der Regel enthält das Feld "Benutzername" zwei Einträge: Ein Eintrag besteht aus dem Namen plus dem Community-Namen, der andere Eintrag besteht aus Vornamen und Nachnamen wie im Fenster "Teilnehmer hinzufügen" des Sametime Administrationswerkzeugs angegeben. Beispiel:

```
Sam Sametime/Acme
Sam Sametime
```

Der Benutzer kann eine der beiden Formen verwenden, wenn er zur Eingabe seines Benutzernamens aufgefordert wird. Sie können auch andere Namen für den Benutzer in das Feld "Benutzername" eingeben. Dem Benutzer stehen dann auch die zusätzlichen Namen für die Anmeldung zur Verfügung.

In einem Benutzernamen können Sie die folgenden Zeichen verwenden: A - Z, 0 - 9, & -._' (Ampersand, Bindestrich, Punkt, Leerzeichen, Unterstrich, Apostroph). Die Verwendung anderer Zeichen kann zu unerwarteten Ergebnissen führen.

Benutzernamen und Internet-Kennwörter unterscheiden Groß- und Kleinschreibung.

**Hinweis** Sie können das Feld "Benutzername" im Personendokument ansehen, indem Sie das Sametime Administrationswerkzeug öffnen, "Benutzer" und dann "Teilnehmer" wählen. Wählen Sie einen Namen aus der Liste, um das Personendokument dieses Benutzers zu öffnen.

## Bearbeiten oder Löschen eines bestehenden Benutzers

Verwenden Sie das Sametime Administrationswerkzeug, um das Personendokument eines Benutzers zu bearbeiten oder den Benutzer aus dem Adreßbuch zu entfernen. Sie können das Internet-Kennwort eines Benutzers ändern, indem Sie sein Personendokument bearbeiten. Durch Löschen seines Personendokuments wird ein Benutzer aus der Sametime Community entfernt. Er kann dann nicht mehr auf Sametime Connect oder geschützte Bereiche des Servers zugreifen.

So bearbeiten oder löschen Sie einen Benutzer:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Administratorname und -kennwort ein, um das Sametime Administrationswerkzeug zu öffnen.
3. Wählen Sie "Benutzer" und dann "Teilnehmer".
4. Doppelklicken Sie auf den Namen des Benutzers, den Sie bearbeiten oder löschen wollen.
5. Um einen Benutzer zu löschen, wählen Sie "Benutzer löschen".

   Um einen Benutzer zu bearbeiten, wählen Sie "Benutzer bearbeiten". Das Personendokument wechselt in den Bearbeitungsmodus, damit Sie beliebige Felder im Personendokument ändern können. Nehmen Sie die gewünschten Änderungen vor.
6. Speichern und schließen Sie das Dokument.

## Verwenden von Gruppendokumenten

Ein Gruppendokument enthält eine Liste von Benutzern, die gemeinsame Züge aufweisen oder dieselben Aufgaben erfüllen. Gruppen sind nützlich zur Verringerung sich wiederholender Aufgaben für Administratoren und Sametime Connect Benutzer.

Benutzer von Sametime Connect Client müssen andere Sametime Benutzer in eine Connect-Liste (oder "Freunde"-Liste) aufnehmen, bevor sie sehen, wer online ist, und mit diesen Benutzern Chats halten können. Wenn Sie ein Gruppendokument mit einer Liste von Benutzern anlegen, kann die gesamte Gruppe einfach in die Connect-Liste aufgenommen werden. Ohne Gruppendokument müssen Sametime Connect Benutzer diese Benutzer einzeln hinzufügen. Sie können beispielsweise ein Gruppendokument mit dem Namen "Technischer Support" anlegen, das alle Angestellten der Abteilung für technischen Support auflistet. Ein Sametime Connect Benutzer kann die Gruppe "Technischer Support" der Connect-Liste hinzufügen, damit er über O
nline-Awareness und Chat-Möglichkeiten mit allen Angestellten des technischen Supports verfügt.

Die Verwendung von Gruppen kann auch administrative Aufgaben vereinfachen. Wenn Sie z. B. die Gruppe "Administratoren" anlegen, die alle Benutzer mit administrativen Aufgaben auflistet, können Sie diese Gruppe in die Zugriffskontrollisten (ACLs) des Sametime Administrationswerkzeugs und des Sametime Adreßbuchs aufnehmen. Wenn Sie einen Administrator hinzufügen wollen, können Sie das Gruppendokument "Administratoren" bearbeiten. Daher brauchen Sie den Namen eines Administrators nur in einer der beiden ACLs (Sametime Administrationswerkzeug oder Sametime Adreßbuch) hinzuzufügen oder zu entfernen, wenn eine entsprechende Änderung erforderlich wird.

Wenn Benutzer für den Zugriff auf das Online-Besprechungszentrum ein Kennwort eingeben sollen, können Sie Gruppendokumente anlegen, um den Zugriff für Besprechungsverwalter und Teilnehmer zu steuern. Erstellen Sie ein Gruppendokument mit dem Namen "Besprechungsverwalter", das alle Benutzer auflistet, die im Online-Besprechungszentrum neue Besprechungen anlegen können. Sie können dann die Gruppe "Besprechungsverwalter" in die ACL des Online-Besprechungszentrums eingeben und der Gruppe Autoren-Zugriff zuweisen. Legen Sie eine weitere Gruppe mit dem Namen "Teilnehmer" an für alle Benutzer, die an Besprechungen teilnehmen, aber keine Besprechungen anlegen dürfen. Weisen Sie der Gruppe "Teilnehmer" im Online-Besprechungszentrum den Leser-Zugriff zu. Sie können nun die Gruppendokumente bearbeiten, um Privilegien für Besprechungsverwalter und -teilnehmer im Online-Besprechungszentrum zu erteilen oder zu entziehen.

**Hinweis** Wenn Sie den Zugriff für Besprechungsverwalter und -teilnehmer über Gruppendokumente steuern, müssen Sie die Einträge "Anonym" und "Standard" in der Datenbank des Online-Besprechungszentrums (STConf.nsf) auf "Kein Zugriff" einstellen. Weitere Informationen finden Sie unter Einstellen grundlegender Kennwortauthentifizierung in einer Datenbank-Zugriffskontrolliste (ACL).

Verwenden Sie das Sametime Administrationswerkzeug, um ein Gruppendokument zu erstellen. Das Gruppendokument wird im Öffentlichen Adreßbuch von Sametime gespeichert. Jede Gruppe muß einen Eigentümer haben. Sie können sich selbst oder einen anderen Administrator als Gruppeneigentümer angeben. Es besteht keine Beschränkung hinsichtlich der Anzahl an Namen, die Sie einer Gruppe hinzufügen können, jedoch sollten Sie umfangreiche Benutzerlisten in zwei oder mehr Untergruppen gliedern, um Ihre Gruppenverwaltung übersichtlicher zu gestalten.

Verwandte Themen anzeigen
Erstellen einer Gruppe
Bearbeiten oder Löschen einer Gruppe

### Erstellen einer Gruppe

Verwenden Sie das Sametime Administrationswerkzeug, um eine Gruppe wie folgt zu erstellen:

1. Wählen Sie im Sametime Administrationswerkzeug "Benutzer" und dann "Gruppen".
2. Klicken Sie auf "Gruppe hinzufügen".
3. Geben Sie einen Namen für die Gruppe in das Feld "Gruppenname" ein (z. B. "Technischer Support", "Besprechungsverwalter" oder "Administratoren").
4. Wählen Sie einen Gruppentyp ("Mehrzweck", "Zugriffskontrolliste" oder "Negativliste"). Gruppen des Typs "Negativliste" werden gewöhnlich verwendet, wenn der Sametime Server mit Lotus Notes Clients und Domino Servern integriert ist.
5. (Optional) Geben Sie eine Beschreibung der Gruppe in das Feld "Beschreibung" ein.
6. Listen Sie die Gruppenmitglieder im Feld "Mitglieder" auf. Geben Sie unbedingt jeden Namen exakt so ein, wie er im Feld "Benutzername" des jeweiligen Personendokuments eingegeben wurde.
7. Geben Sie die Namen der Gruppeneigentümer in das Feld "Eigentümer" ein.
8. Speichern und schließen Sie das Dokument.

Verwandte Themen anzeigen
Details: Erstellen einer Gruppe

### Details: Erstellen einer Gruppe

Als Teil der Gruppendefinition können Sie je nach Einsatz der Gruppe einen Gruppentyp zuweisen. Damit wird die Größe der Adreßbuch-Indizes verringert und die Leistung verbessert, und Sie verfügen über zusätzliche Informationen über den Grund der Gruppenbildung.

Verwenden Sie den Typ "Mehrzweck" für Sametime Connect Gruppen und Administrationsgruppen. Verwenden Sie einen speziellen Gruppentyp, z. B. "Nur Zugriffskontrolliste", wenn Sie eine Gruppe für einen bestimmten Zweck nutzen.

### Bearbeiten oder Löschen einer Gruppe

Verwenden Sie das Sametime Administrationswerkzeug, um eine Gruppe wie folgt zu bearbeiten oder zu löschen:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Administratorname und -kennwort ein, um das Sametime Administrationswerkzeug zu öffnen.
3. Wählen Sie "Benutzer" und dann "Gruppe".
4. Klicken Sie auf den Namen der Gruppe, die Sie bearbeiten oder löschen wollen.
5. Um eine Gruppe zu löschen, wählen Sie "Gruppe löschen". Das Gruppendokument wird entfernt und Sie kehren zur Ansicht "Gruppen" zurück.

   Um eine Gruppe zu bearbeiten, wählen Sie "Gruppe bearbeiten" und nehmen Sie die gewünschten Änderungen vor. Speichern und schließen Sie das Dokument.

## Verwenden der Funktion "Selbstregistrierung"

Der Sametime Server umfaßt eine Funktion zur Selbstregistrierung. Mit Hilfe dieser Funktion kann ein Benutzer ein Personendokument im Adreßbuch anlegen, das seinen Benutzernamen und sein Internet-Kennwort enthält. Die Selbstregistrierung wird unterstützt, wenn Sametime in einer reinen Web-Umgebung installiert ist. Diese Funktion steht Lotus Notes Benutzern nicht zur Verfügung und wird ebenfalls nicht unterstützt, wenn Sametime in einer Domino Umgebung installiert ist.

Selbstregistrierung ist standardmäßig nach der Installation gestattet, aber der Administrator kann die Selbstregistrierung aus Sicherheitsgründen verbieten. Durch Selbstregistrierung kann sich der Administrationsaufwand verringern, da Benutzer sich selbst in das Sametime Adreßbuch aufnehmen können.

Die Selbstregistrierung kann für einige Unternehmen ein Sicherheitsrisiko darstellen, da sie jedem Benutzer, der mit einem Web-Browser auf den Server zugreift, folgendes gestattet:

- Hinzufügen von Personendokumenten zum Adreßbuch
- Verwenden von Sametime Connect
- Zugriff auf geschützte Bereiche des Servers mit einem Web-Browser

Wenn Benutzer mit diesen Möglichkeiten eine Gefahr für die Sicherheit Ihres Unternehmens darstellen, siehe Verwenden der Selbstregistrierung, um diese Funktion zu deaktivieren.

Hinweis   Das Sametime Adreßbuch muß den Dateinamen NAMES.NSF besitzen, damit die Selbstregistrierung problemlos funktioniert.

Verwandte Themen anzeigen
Verwenden der Selbstregistrierung

## Verwalten von Benutzern in einer Notes/Domino Umgebung

Das Sametime Administrationswerkzeug ist das empfohlene Administrationswerkzeug für den Sametime Server. Wenn Sie jedoch Sametime in einer Domino Umgebung installiert haben, beachten Sie folgende Punkte beim Hinzufügen von Benutzern mit dem Sametime Administrationswerkzeug:

- Beim Hinzufügen eines Benutzers mit dem Sametime Administrationswerkzeug wird ein Personendokument mit einem Internet-Kennwort für diesen Benutzer in das Adreßbuch auf dem Sametime Server eingefügt. Eine Notes Benutzer-ID wird jedoch nicht angelegt.
- Wenn Benutzer auf den Sametime Server mit einem Notes Client zugreifen sollen und ein Benutzer noch nicht in der Domäne registriert ist, führen Sie die übliche Domino Prozedur für das Registrieren eines neuen Benutzers aus. Verwenden Sie einen Notes Client, um den Benutzer in einem Domino Adreßbuch auf einem Domino Server zu registrieren. Geben Sie dem Benutzer unbedingt ein Internet-Kennwort. Das Internet-Kennwort ist erforderlich, um auf den Sametime Connect Client zuzugreifen. Außerdem muß das Adreßbuch, in dem der neue Benutzer registriert wird, ein Adreßbuch sein, das auf dem Sametime Server repliziert wird.

  Bei der Installation in einer Domino Umgebung, in der Domino Server in einer älteren Version als 4.6.5 läuft, wird das Adreßbuch auf dem Server geändert, auf dem Sametime läuft. Unabhängig davon, ob Sie Sametime auf einem eigenen Server oder einem Server mit Domino installieren, sollten Sie verhindern, daß das Adreßbuch vom Sametime Server auf die Domino Server in der Domäne repliziert wird. In diesem Fall erscheinen Benutzer, die dem Sametime Adreßbuch hinzugefügt werden, nicht in den Adreßbüchern auf anderen Domino Servern in der Domäne.

  Bei der Installation in einer Domino Umgebung, in der Domino Server mit der Domino Server Version 4.6.5 oder höher laufen, werden alle von Sametime verlangten Adreßbuch-Designänderungen in das Domino Release integriert. Die Replizierung des Adreßbuchs von einem Server, auf dem Sametime läuft, auf die Domino Server sollte problemlos verlaufen. Installationsanleitungen finden Sie im *Sametime Installationshandbuch*.
- Selbstregistrierung wird nicht unterstützt, wenn Sametime 1.5 in einer Domino Umgebung installiert ist.

Verwandte Themen anzeigen
Verwalten von Sametime Benutzern

# Kapitel 04: Konfigurieren von Anschlüssen und Netzwerkeinstellungen

## Einstellungen für Sametime Anschlüsse und Netzwerk

Dieser Abschnitt beschreibt die Netzwerkanschlüsse, die der Sametime Server verwendet, sowie die Netzwerk-Konfigurationseinstellungen, die im Sametime Administrationswerkzeug verfügbar sind.

**Sametime Community Server**
Der Sametime Community Server umfaßt Netzwerkeinstellungen, die Verbindungen vom Sametime Connect Client unterstützen. Diese Einstellungen befinden sich unter "Community Services Netzwerk" auf der Administrationsseite "Netzwerk und Sicherheit" (verfügbar im Sametime Administrationswerkzeug). Diese Netzwerkeinstellungen beinhalten Anschlüsse für die folgenden Verbindungstypen:

- Direkte TCP/IP-Verbindungen
- SOCKS-Proxy-Verbindungen
- HTTPS-Verbindungen
- HTTP-Verbindungen (nur möglich, wenn der Administrator HTTP-Proxy-Tunneling für den Community Server aktiviert)

Weitere Informationen über Verbindungsprozeß und Verbindungseinstellungen von Sametime Connect Client sowie die Community Services Netzwerkeinstellungen finden Sie unter Verbindung zum Community Server in der vorliegenden Dokumentation.

**Sametime Besprechungsserver**
Der Sametime Besprechungsserver besitzt Anschluß- und Netzwerkeinstellungen, die Verbindungen von den Client Java-Applets und der OCX- Komponente "Anwendung gemeinsam nutzen" unterstützen. Diese Einstellungen befinden sich unter "Meeting Services Netzwerk" der Administrationsseite "Netzwerk und Sicherheit" (verfügbar im Sametime Administrationswerkzeug). Der Sametime Besprechungsserver unterstützt die folgenden Verbindungstypen für die Komponente "Anwendung gemeinsam nutzen" und die Client-Java-Applets:

- Direkte TCP/IP-Verbindungen
- SOCKS-Proxy-Verbindungen
- HTTPS-Verbindungen (nicht unterstützt für die Client Java-Applets)
- HTTP-Verbindungen

Weitere Informationen über den Verbindungsprozeß von Client-Java-Applets und der Komponente "Anwendung gemeinsam nutzen" sowie über die Netzwerkeinstellungen der Sametime Meeting Services finden Sie unter Verbindung mit dem Online-Besprechungsserver in der vorliegenden Dokumentation.

Verwandte Themen anzeigen
Vom Sametime Server verwendete Anschlüsse

## Vom Sametime Server verwendete Anschlüsse

Komponenten des Sametime Servers verwenden bestimmte TCP/IP-Anschlüsse, um eingehende Anfragen zu erkennen. Mit Hilfe des Sametime Administrationswerkzeugs können Sie die Anschlüsse konfigurieren, die die Komponenten des Sametime Servers nutzen.

Wenn Sie das Sametime Administrationswerkzeug öffnen, sind die Einstellungen für Netzwerkanschlüsse und -Tunneling sofort sichtbar. Im Sametime Administrationswerkzeug können Sie "Server" und dann "Netzwerk und Sicherheit" wählen, um die Netzwerkeinstellungen anzusehen und zu ändern.

Nachstehende Tabelle listet die Standardanschlüsse auf, die der Sametime Server verwendet. Die meisten dieser Anschlüsse sind konfigurierbar.

| Standard-anschluß | Verwenden Sie |
|---|---|
| 80 | Der Sametime HTTP-Server wartet an diesem Anschluß auf eingehende HTTP-Anfragen. |
| 1080 | Der Community Server wartet an diesem Anschluß auf SOCKS-Proxy-Verbindungen. |

| | |
|---|---|
| 1516 | Der Community Server wartet an diesem Anschluß auf Verbindungen von den Community Server Komponenten anderer Sametime Server. |
| 1533 | Der Community Server wartet an diesem Anschluß auf direkte TCP/IP-Verbindungen von den Community Server Clients. Dies ist ein bekannter Anschluß für Sametime Community Server-Client-Verbindungen.<br>Standardmäßig wartet der Community Server an diesem Anschluß auch auf HTTPS-Verbindungen. Der HTTPS-Anschluß des Community Servers unterstützt Sametime Connect Clients, die über einen HTTPS-Proxy eine Internet-Verbindung aufbauen. |
| 8082 | Der Community Server wartet an diesem Anschluß auf HTTP-Verbindungen, wenn der Administrator HTTP-Tunneling-Unterstützung für den Community Server aktiviert. Dieser Anschluß unterstützt Community Server Clients, die über einen HTTPS-Proxy eine Internet-Verbindung aufbauen. |
| 1503 | Der Besprechungsserver wartet an diesem Anschluß auf T.120-Verbindungen von der Komponente "Besprechungsserver" anderer Sametime Server. Der Besprechungsserver wartet an diesem Anschluß auch auf T.120-Verbindungen von Microsoft NetMeeting Clients.<br>Diese Anschlußnummer bezeichnet den registrierten Anschluß für T.120-Anwendungen, die TCP/IP verwenden. Sie können einen anderen Anschluß für die T.120-Verbindungen festlegen. |
| 8081 | Der Besprechungsserver wartet an diesem Anschluß auf direkte TCP/IP-, HTTP- und HTTPS-Verbindungen vom Besprechungsserver.<br>HTTPS-Verbindungen werden nur für die Komponente "Anwendung gemeinsam nutzen" unterstützt. |
| 443 | Der Sametime HTTP-Server wartet an diesem Anschluß auf Secure Sockets Layer- (SSL oder HTTPS) Verbindungen von Web-Browsern. Um den HTTP-Server so zu konfigurieren, daß er auf diese Verbindungen wartet, müssen Sie den SSL-Anschluß im Abschnitt Internetanschluß- und Sicherheitskonfiguration des Serverdokuments aktivieren. |

Verwandte Themen anzeigen
Einstellungen für Sametime Anschlüsse und Netzwerk

## Sametime HTTP-Serveranschluß

Der Sametime Server enthält einen eigenen HTTP Web Server. Web-Browser greifen auf den Sametime Server über den HTTP-Serveranschluß zu, der auf der Administrationsseite "Netzwerk und Sicherheit" (verfügbar im Sametime Administrationswerkzeug) aktiviert ist. Die Standard-Anschlußnummer für den HTTP-Web-Server ist 80.

Der HTTP-Serveranschluß ist konfigurierbar. Um auf die Einstellung des HTTP-Serveranschlusses zuzugreifen, öffnen Sie das Sametime Administrationswerkzeug und wählen Sie "Server - Netzwerksicherheit".

Verwandte Themen anzeigen
Vom Sametime Server verwendete Anschlüsse
Einstellungen für Sametime Anschlüsse und Netzwerk

## Verbindung zum Sametime Community Server

Dieser Abschnitt behandelt Sametime Connect Client-Verbindungen zum Sametime Community Server.

Der Community Server unterstützt die Funktionen für Online-Awareness, sofortige Nachrichten und Gruppen-Chat des Sametime Connect Clients. Der Sametime Connect Client muß mit dem Sametime Community Server verbunden sein, damit diese Funktionen verfügbar sind.

Die Firewall-Konfiguration des Benutzers beeinflußt die Art der Verbindung zwischen Sametime Connect Client und Sametime Community Server. Der Benutzer muß evtl. die Verbindungseinstellungen des Sametime Connect Clients ändern, um die Firewall-Konfiguration zu berücksichtigen. Weitere Informationen finden Sie unter Sametime Verbindungsoptionen für den Sametime Connect Client.

**Hinweis** Der Sametime Connect Client umfaßt auch Verbindungsoptionen, über die eine Verbindung zu einem America Online (AOL®) Instant Messenger℠ Server möglich ist. Weitere Informationen finden Sie unter AOL Instant Messenger Verbindungseinstellungen für den Sametime Connect Client.

Der Sametime Server unterstützt die folgenden Verbindungstypen vom Sametime Connect Client zum Sametime Community Server:

- **Direkte TCP/IP-Verbindung** - Wird verwendet, wenn der Sametime Connect Client nicht über einen Proxy-Server mit dem Internet verbunden wird.
- **HTTPS-Verbindung** - Wird verwendet, wenn der Sametime Connect Client über einen HTTPS-Proxy-Server mit dem Internet verbunden wird.
- **HTTP-Verbindung** - Wird verwendet, wenn der Sametime Connect Client über einen HTTP-Proxy-Server mit dem Internet verbunden wird. Damit diese Art von Verbindung erfolgreich ist, muß der Sametime Administrator die HTTP-Tunneling-Unterstützung in den Einstellungen "Netzwerk und Sicherheit" des Sametime Administrationswerkzeugs aktivieren.
- **SOCKS-Verbindung** - Wird verwendet, wenn der Sametime Connect Client über einen SOCKS-Proxy-Server mit dem Internet verbunden wird.

Der Sametime Community Server erwartet die unterschiedlichen Verbindungstypen auf dem jeweils entsprechenden Anschluß. Die meisten dieser Anschlüsse sind konfigurierbar. Sie können auf die Einstellungen des Community Serveranschlusses über die Seite "Netzwerk und Sicherheit" des Sametime Administrationswerkzeugs zugreifen. Weitere Informationen finden Sie unter Netzwerkeinstellungen des Community Servers.

Verwandte Themen anzeigen
Verbindungsprozeß des Sametime Connect Clients
Sametime Verbindungseinstellungen für den Sametime Connect Client
Community Services Netzwerkeinstellungen
Vom Sametime Server verwendete Anschlüsse

## Verbindungsprozeß des Sametime Connect Clients

Der Verbindungsprozeß des Sametime Connect Clients wird durch folgendes gesteuert:

- Verbindungseinstellungen im Sametime Connect Client
- Anschlußeinstellungen des Sametime Community Servers in der Seite "Netzwerk und Sicherheit" (verfügbar im Sametime Administrationswerkzeug)
- Firewall-Konfigurationen von Client und Server

Nachstehende Schritte beschreiben den Verbindungsprozeß für den Sametime Connect Client.

1. Der Endbenutzer öffnet den Sametime Connect Client.
2. Der Sametime Connect Client baut eine Verbindung zum Sametime Community Server auf, der in den Verbindungseinstellungen des Sametime Connect Clients angegeben ist. (Diese Einstellungen stehen im Sametime Connect Client über "Optionen - Vorgaben - Sametime Anschlußmöglichkeit" zur Verfügung.)
3. Der Verbindungstyp und der verwendete Anschluß für die Verbindung mit dem Community Server hängt von folgenden Verbindungseinstellungen im Sametime Connect Client ab:

**Sametime Community Serveranschluß** - Der Standardanschluß ist 1533. Der angegebene Sametime Community Serveranschluß muß für eine erfolgreiche Verbindung mit dem Sametime Community Server für abgehende Verbindungen an der Firewall des Clients geöffnet sein. Der Sametime Community Server muß sich entweder außerhalb einer Firewall befinden oder Verbindungen durch die Firewall am Sametime Community Serveranschluß gestatten, damit die Verbindung erfolgreich sein kann.

**Proxy-Typ** - Die Standardeinstellung für den Sametime Connect Client (und für die Komponente "Anwendung gemeinsam nutzen") lautet "Kein Proxy". Mit dieser Einstellung versucht der Client eine direkte TCP/IP-Verbindung zum Server über den Sametime Community Serveranschluß. Der Server wartet auf diese Verbindung am "Community Serveranschluß für Client-Verbindungen" (Anschluß 1533).

Wenn der Sametime Connect Client über einen Proxy-Server auf das Internet zugreifen soll, muß der Benutzer den geeigneten Proxy-Typ in den Verbindungseinstellungen des Sametime Connect Clients wählen. Wenn der Benutzer z. B. über einen HTTPS-Proxy-Server auf das Internet zugreift, wählt er in den Verbindungseinstellungen des Sametime Connect Clients die Option "HTTPS-Proxy verwenden". Der Community Server wartet auf diese Verbindung an dem Anschluß, der auf der Seite "Netzwerk und Sicherheit" (verfügbar im Sametime Administrationswerkzeug) als Community Services HTTPS-Anschluß festgelegt ist.

Für eine erfolgreiche Verbindung mit dem Sametime Community Server muß die Anschlußnummer des Sametime Community Servers im Sametime Connect Client dem Anschluß entsprechen, der für das Verbindungsprotokoll auf dem Server angegeben ist (direkte Verbindung, HTTP oder HTTPS).

Verwandte Themen anzeigen

Sametime Verbindungseinstellungen für den Sametime Connect Client
Community Services Netzwerkeinstellungen

## Sametime Verbindungseinstellungen für den Sametime Connect Client

Wenn ein Client über einen Proxy-Server mit dem Community Server verbunden wird, muß der Benutzer evtl. die Verbindungseinstellungen von Sametime Connect ändern. Sobald der Benutzer diese Einstellungen definiert hat, sind spätere Änderungen erst dann erforderlich, wenn sich die Proxy- oder Firewall-Konfiguration des Benutzers ändert.

Der Benutzer kann Verbindungseinstellungen über das Register "Optionen - Vorgaben - Sametime Anschlußmöglichkeit" des Sametime Connect Clients ändern.

**Hinweis** Die Komponente "Anwendung gemeinsam nutzen" umfaßt ebenfalls Verbindungseinstellungen. Die Verbindungseinstellungen des Sametime Connect Clients und der Komponente "Anwendung gemeinsam nutzen" werden beide in der Sametime Connect Datei connect.ini im Verzeichnis C:\Program Files\Lotus\Sametime Client auf dem lokalen Computer des Benutzers gespeichert. Wenn der Benutzer die Verbindungsoptionen für einen dieser Clients festlegt, verwendet der andere automatisch dieselben Einstellungen.

Die Verbindungseinstellungen des Sametime Connect Clients:

- **Host** - Der Sametime Connect Client baut eine Verbindung zum in diesem Feld angegebenen Sametime Community Server auf.
- **Anschluß** - Der Sametime Connect Client versucht die Verbindung zum Community Server über den in diesem Feld angegebenen Community Serveranschluß.**Anschluß für gemeinsam genutzte Anwendung** - Dieser Anschluß wird verwendet, wenn ein Benutzer die Komponente "Anwendung gemeinsam nutzen" von Sametime Connect startet. Weitere Informationen finden Sie unter Verbindungen von der Komponente "Anwendung gemeinsam nutzen" mit dem Online-Besprechungsserver.
- **Kein Proxy** - Der Benutzer wählt diese Option, wenn der Internet-Zugriff nicht über einen Proxy-Computer erfolgt. Wenn diese Option aktiviert ist, baut der Sametime Connect Client über Anschluß 1533 eine direkte Verbindung zum Community Server auf.

  Der Community Server wartet am "Community Serveranschluß für Client-Verbindungen" (Anschluß 1533) auf diese Verbindung.
- **SOCKS-Proxy verwenden** - Der Benutzer wählt diese Option, wenn der Internet-Zugriff über einen SOCKS-Proxy erfolgt. Wenn diese Option aktiviert ist, baut der Sametime Connect Client über den "Community Serveranschluß für direkte Client-Verbindungen" (Anschluß 1533) eine SOCKS-Verbindung zum Sametime Server auf.

Wenn der Benutzer diese Option wählt, muß er den DNS-Namen oder die IP-Adresse des SOCKS-Proxy-Servers und den Anschluß für den SOCKS-Proxy-Server angeben. Wenn die Verbindung über einen SOCKS5-Proxy erfolgt, muß der Benutzer auch seinen SOCKS-Benutzernamen und sein SOCKS-Kennwort eingeben.

- **HTTPS-Proxy verwenden** - Der Benutzer wählt diese Option, wenn der Internet-Zugriff über einen HTTPS-Proxy erfolgt. Der Verbindungsversuch erfolgt über den Anschluß, der in den Sametime Connect Verbindungsoptionen als Community Serveranschluß angegeben ist.

  Der Community Server wartet am "Community Server HTTPS-Anschluß" auf HTTPS-Verbindungen. Dieser Anschluß ist in den Einstellungen unter "Netzwerk und Sicherheit" im Sametime Administrationswerkzeug auch auf Anschluß 1533 eingestellt.

  Wenn HTTPS-Proxy als Proxy-Typ gewählt ist, muß die Einstellung des Community Serveranschlusses mit der des Community Server HTTPS-Anschlusses in den Administrationseinstellungen unter "Netzwerk und Sicherheit" auf dem Server übereinstimmen.

- **HTTP-Proxy verwenden** - Der Benutzer wählt diese Option, wenn der Internet-Zugriff über einen HTTP-Proxy erfolgt. Der Sametime Administrator muß für den Community Server die Option "HTTP-Tunneling-Unterstützung" aktivieren, damit diese Verbindung erfolgreich ist. Weitere Informationen finden Sie unter Community Services Netzwerkeinstellungen.

  Der HTTP-Verbindungsversuch erfolgt über den Anschluß, der in den Sametime Connect Verbindungsoptionen als Community Serveranschluß festgelegt ist. Der Community Server wartet am "HTTP-Tunneling-Anschluß" auf HTTP-Verbindungen. Standardmäßig ist dieser Anschluß auf 8082 gesetzt.

  Wenn HTTP-Proxy als Proxy-Typ gewählt ist, muß die Einstellung des Community Serveranschlusses mit der des Community Server HTTP-Tunneling-Anschlusses am Sametime Server übereinstimmen. Wenn z. B. der HTTP-Tunneling-Anschluß am Server auf 8082 eingestellt ist, muß auch der Community Serveranschluß am Sametime Connect Client Community Server auf 8082 eingestellt sein.

Verwandte Themen anzeigen
Verbindungsprozeß des Sametime Connect Clients

## Community Services Netzwerkeinstellungen

Der Community Server umfaßt die folgenden Netzwerkanschluß- und -Tunneling-Optionen. Auf diese Einstellungen greifen Sie im Sametime Administrationswerkzeug zu, indem Sie "Server" und dann "Netzwerk und Sicherheit" wählen.

**Community Serveranschluß für Client-Verbindungen**
Der Community Serveranschluß für Client-Verbindungen wartet auf direkte Verbindungen von den Sametime Connect Clients. Der Community Server wartet auch auf Verbindungen von den Funktionen "Wer ist online" und "Wer ist anwesend" einer Sametime-aktivierten Datenbank. Dieser Anschluß ist auf 1533 eingestellt und kann nicht geändert werden.

**Community Serveranschluß für Serververbindungen**
Der Community Serveranschluß für Serververbindungen wartet auf Verbindungen von der Community Server Komponente anderer Sametime Server, wenn mehrere Sametime Server in einer Domino Umgebung installiert sind.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**HTTPS-Anschluß des Community Servers**
Der HTTPS-Anschluß des Community Servers wartet auf HTTPS-Verbindungen vom Sametime Connect Client. Dieser Anschluß ermöglicht Clients, die über einen HTTPS-Proxy auf das Internet zugreifen, die Verbindung zum Community Server. Der HTTPS-Standardanschluß des Community Servers HTTPS ist 1533.

Der Sametime Connect Client versucht am HTTPS-Anschluß des Community Servers eine HTTPS-Verbindung zum Community Server, wenn der Benutzer die Option "HTTPS-Proxy verwenden" unter den Verbindungseinstellungen des Sametime Connect Clients gewählt hat.

Wenn Sie diese Anschlußnummer ändern, müssen auch Sametime Connect Clients, die über einen HTTPS-Proxy-Server auf das Internet zugreifen, den Anschluß ändern, der unter den Verbindungseinstellungen des Sametime Connect Clients als Community Serveranschluß angegeben ist. Die Einstellung für den Client- und den HTTPS-Anschluß muß übereinstimmen, damit die Verbindung erfolgen kann.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**Hinweis** Daten, die über den Community Server HTTPS-Anschluß übertragen werden, sind nicht verschlüsselt.

**HTTP-Tunneling-Unterstützung**
Mit Hilfe der HTTP-Tunneling-Unterstützung des Community Servers können Sametime Connect Clients, die über einen HTTP-Proxy auf das Internet zugreifen, eine Verbindung mit dem Community Server aufbauen. Wenn HTTP-Tunneling-Unterstützung aktiviert ist, wartet der Community Server am HTTP-Tunneling-Anschluß auf HTTP-Verbindungen. Wenn die Tunneling-Unterstützung deaktiviert ist, können Sametime Connect Clients über einen HTTP-Proxy keine Verbindung zum Community Server aufbauen.

**HTTP-Tunneling-Anschluß**
Der HTTP-Anschluß des Community Servers wartet auf HTTP-Verbindungen vom Sametime Connect Client, wenn die HTTP-Tunneling-Unterstützung eingeschaltet ist. Dieser Anschluß ermöglicht Clients, die über einen HTTP-Proxy auf das Internet zugreifen, eine Verbindung zum Community Server aufzubauen. Der HTTP-Tunneling-Standardanschluß ist 8082.

Der Sametime Connect Client versucht eine HTTP-Verbindung zum Community Server am HTTP-Tunneling-Anschluß des Community Servers, wenn der Benutzer die Option "HTTP-Proxy verwenden" in den Verbindungseinstellungen des Sametime Connect Clients wählt.

Wenn Sie diese Anschlußnummer ändern, müssen auch Sametime Connect Clients, die über einen HTTP-Proxy-Server auf das Internet zugreifen, den Anschluß ändern, der unter den Verbindungseinstellungen des Sametime Connect Clients als Community Serveranschluß angegeben ist. Die Einstellung für den Client-Anschluß und den HTTP-Anschluß am Server muß übereinstimmen, damit die Verbindung erfolgen kann.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung

Verwandte Themen anzeigen

Verbindungsprozeß des Sametime Connect Clients
Sametime Verbindungseinstellungen für den Sametime Connect Client
Verbindung zum Sametime Community Server

## AOL Instant Messenger Verbindungseinstellungen für den Sametime Connect Client

Der Sametime Connect Client erlaubt einem Sametime Benutzer die Kommunikation mit Personen, die bei America Online (AOL) und dem AOL Instant Messenger Server angemeldet sind. Um mit AOL-Benutzern zu kommunizieren, muß der Sametime-Benutzer:

- bei America Online registriert sein
- eine Verbindung zu einem AOL Instant Messenger Server aufbauen, indem er die Verbindungseinstellungen von AOL Instant Messenger im Sametime Connect Client festlegt. (Anleitungen hierzu finden Sie auf dieser Seite unter "Verbindungsoptionen für AOL Instant Messenger festlegen".)

Sametime Connect unterstützt mehrere Verbindungsarten zum AOL Instant Messenger Server. Der Benutzer kann eine direkte TCP/IP-Verbindung verwenden oder, falls sich der Server außerhalb einer Firewall befindet, einen Proxy-Server oder eine direkte TCP/IP-Verbindung (falls die Firewall dies gestattet). Dem Benutzer stehen folgende Arten der Verbindung zum Community Server zur Verfügung:

- **Direkte TCP/IP-Verbindung ohne Proxy.** Wenn sich der Sametime Community Server außerhalb einer Firewall befindet, muß der Benutzer in der Lage sein, auf Services an Anschluß 5190 (der bekannte Anschluß von AOL Instant Messenger) zuzugreifen. Anschluß 5190 muß für abgehende TCP/IP-Verbindungen geöffnet sein.
- **HTTPS-Proxy-Server**
- **SOCKS-Proxy-Server**

Die nachstehenden Themen beschreiben die Prozeduren für AOL Instant Messenger Verbindungen, die von Sametime Connect aus aufgebaut werden. Diese Prozeduren führt der Endbenutzer am Sametime Connect Client aus.

### Verbindungsoptionen für AOL Instant Messenger festlegen

1. Wählen Sie im Sametime Connect Client "Optionen - Vorgaben".
2. Klicken Sie auf "AOL Instant Messenger Anschlußmöglichkeit ".
3. Geben Sie den Hostnamen des AOL Instant Messenger Servers sowie die Anschlußnummer ein.
4. Wählen Sie die geeignete Option für den Proxy-Typ:
   - Wenn Ihr Unternehmen keinen Proxy-Server einsetzt, wählen Sie "Kein Proxy".
   - Wenn Ihr Unternehmen einen HTTPS-Proxy einsetzt, wählen Sie "HTTPS-Proxy" und geben Sie den Servernamen und die Anschlußnummer für den Proxy an. Die Standard-Anschlußnummer ist 80.

   **Hinweis** Bei HTTPS-Proxies ist die Anschlußnummer für AOL Instant Messenger standardmäßig 443.

   - Wenn Ihr Unternehmen einen SOCKS-Proxy einsetzt, befolgen Sie nachstehende Anleitungen, um eine SOCKS-Proxy-Verbindung zu konfigurieren.
5. Klicken Sie auf OK, um Ihre Änderungen zu speichern.

### Eine SOCKS-Proxy-Verbindung konfigurieren

1. Wählen Sie im Register "Sametime Connect AOL Instant Messenger Anschlußmöglichkeit " die Option "SOCKS-Proxy verwenden".
2. Geben Sie den Hostnamen und die Anschlußnummer des Proxy-Servers in den Bereich "Proxy-Server" ein. Die Standard-Anschlußnummer ist 1080.
3. Wählen Sie im Bereich "Authentifizierung" die Option "Socks4" oder "Socks5".
4. (Nur für Socks5-Proxies) Geben Sie Ihren SOCKS-Benutzernamen und Ihr Kennwort ein.
5. Klicken Sie auf OK, um Ihre Änderungen zu speichern.

### Den Servernamen von AOL Instant Messenger ändern

1. Geben Sie im Register "Sametime Connect AOL Instant Messenger Anschlußmöglichkeit" den neuen Hostnamen für den AOL Instant Messenger Server ein.
2. Klicken Sie auf OK.
3. Wählen Sie "Teilnehmer - Anmelden", um sich beim neu definierten AOL Instant Messenger Server anzumelden.

## Verbindung zum Sametime Besprechungsserver

Dieser Abschnitt behandelt Client-Verbindungen zum Sametime Besprechungsserver. Informationen über Serververbindungen zum Besprechungsserver finden Sie unter Verwenden mehrerer Sametime Server.

Die folgenden beiden Client-Komponenten können eine Verbindung zum Sametime Besprechungsserver aufbauen:

- **Client-Java-Applets** - Diese Applets umfassen den Betrachter für gemeinsam genutzte Anwendungen und die Pinwand. Die Applets werden automatisch auf einen Web-Browser oder Lotus Notes heruntergeladen, wenn der Benutzer an einer Online-Besprechung teilnimmt.

  Die Client-Java-Applets müssen eine Verbindung zur Sametime Besprechungsserver-Komponente aufbauen, damit sie in einer Online-Besprechung funktionieren. Für diese Applets erfolgen direkte TCP/IP-, HTTP-Proxy-Tunneling- und SOCKS-Verbindungen zum Besprechungsserver automatisch. Für diese Verbindungen ist keine Client-Konfiguration erforderlich.
- **OCX-Komponente "Anwendung gemeinsam nutzen"** - Diese Komponente ist Teil des Sametime Client Pakets und läuft als separate Anwendung auf dem lokalen Computer des Benutzers. Der Benutzer startet die Komponente "Anwendung gemeinsam nutzen", um eine auf seinem lokalen Computer installierte Anwendung gemeinsam mit entfernten Teilnehmern einer Online-Besprechung zu nutzen.

Der Benutzer kann den OCX-Client "Anwendung gemeinsam nutzen" während einer Online-Besprechung im Online-Besprechungszentrum vom Client-Java-Applet oder vom Sametime Connect Client aus starten.

Der OCX-Client "Anwendung gemeinsam nutzen" muß eine Verbindung zur Sametime Besprechungsserver-Komponente aufbauen, damit er in einer Online-Besprechung funktioniert.

Der Sametime Besprechungsserver unterstützt direkte TCP/IP-, SOCKS-Proxy-, HTTP- und HTTPS-Verbindungen vom OCX-Client "Anwendung gemeinsam nutzen".

Der Benutzer muß die OCX-Komponente "Anwendung gemeinsam nutzen" manuell konfigurieren, wenn er über einen Proxy auf das Internet zugreift. Der Benutzer nimmt diese Konfigurationseinstellungen in den Verbindungsoptionen vor, die im OCX-Client "Anwendung gemeinsam nutzen" zur Verfügung stehen.

Verwandte Themen anzeigen

Java-Applet-Verbindungen zum Besprechungsserver
Verbindungen von der Komponente "Anwendung gemeinsam nutzen" zum Besprechungsserver
Verbindungseinstellungen für die Komponente "Anwendung gemeinsam nutzen"

## Java-Applet-Verbindungen zum Besprechungsserver

Die Client-Java-Applets (Betrachter für gemeinsam genutzte Anwendungen und Pinwand) müssen eine Verbindung zur Besprechungsserver-Komponente des Sametime Servers aufbauen, damit ein Benutzer an der gemeinsamen Nutzung einer Anwendung oder einer Pinwand-Besprechung teilnehmen kann.

Der Sametime Server unterstützt eine direkte TCP/IP-Verbindung von den Client-Java-Applets zum Besprechungsserver. Der Sametime Server bietet auch SOCKS-Proxy- und HTTP-Proxy-Unterstützung für die Java-Applet-Verbindungen zum Besprechungsserver.

Die Firewall-Konfiguration des Clients beeinflußt die Verbindungsmethode der Java-Applets.

Die folgenden Szenarien erklären Verbindungen vom Java-Applet zum Besprechungsserver.

**Direkte Java-Applet-Verbindungen und SOCKS-Proxy-Verbindungen zum Besprechungsserver**

Wenn ein Benutzer an einer Online-Besprechung teilnimmt, wird ein Java-Applet auf den Client heruntergeladen. Das Client-Java-Applet versucht eine direkte TCP/IP-Verbindung zum Besprechungsserver über den Anschluß, der für den Besprechungsserver in den Meeting Services Netzwerkeinstellungen angegeben ist (standardmäßig 8081).

So erfolgt der direkte Verbindungsprozeß für Java-Applets:

1. Ein Client greift auf die Anwendung Online-Besprechungszentrum (STConf.nsf) zu. Der Client kann ein Web-Browser (Internet Explorer 4.x oder Netscape Navigator 4.06) oder Lotus Notes (4.6.2 oder höher) sein.
2. In der Anwendung Online-Besprechungszentrum versucht der Benutzer, an einer Online-Besprechung teilzunehmen. Ein Java-Applet wird auf den Client heruntergeladen. Das Java-Applet versucht eine direkte Verbindung zum Besprechungsserver über den Anschluß, der für den Besprechungsserver festgelegt ist (standardmäßig 8081).

   Wenn der Client über einen SOCKS-Proxy auf das Internet zugreift, verwendet das Java-Applet die SOCKS-Proxy-Dienste, um über den für den Besprechungsserver angegebenen Anschluß (standardmäßig 8081) eine Verbindung zum Besprechungsserver aufzubauen.

   Mit Internet Explorer leitet die virtuelle Browser-Maschine die Verbindung durch den SOCKS-Proxy. Internet Explorer verwendet seine eigenen SOCKS-Proxy-Konfigurationseinstellungen für diese Verbindungsmethode. Netscape-Browser verwenden das HTTP-Tunneling-Protokoll durch den Browser.
3. Diese Verbindung ist nur erfolgreich, wenn die Firewall des Clients abgehende Verbindungen am Besprechungsserver-Anschluß (8081) erlaubt.

   Wenn die Firewall des Clients abgehende Verbindungen am Besprechungsserver-Anschluß (8081) blockiert, versucht das Java-Applet Tunneling durch einen HTTP-Proxy-Server. Dieses Verbindungsszenario wird nachstehend beschrieben.

**HTTP-Proxy-Tunneling vom Java-Applet zum Besprechungsserver**

HTTP-Proxy-Tunneling zum Besprechungsserver tritt ein, wenn die direkte Verbindung fehlschlägt. Clients, die eine Verbindung über HTTP-Proxy-Tunneling aufbauen, müssen mit einer geringeren Leistung während der Besprechung rechnen als Clients, die direkt oder durch einen SOCKS-Proxy verbunden sind.

1. Das Client-Java-Applet versucht (wie oben beschrieben) eine direkte Verbindung durch den Besprechungsserver-Anschluß, aber die Firewall des Clients blockiert die direkte Verbindung.
2. Mit Hilfe des vom Server heruntergeladenen Codes bettet der Client den Hostnamen des Sametime Servers und die für die Verbindung erforderlichen Daten in eine HTTP-Anfrage ein.
3. Diese Anfrage wird durch den HTTP-Proxy des Clients an den Besprechungsserver gesendet. Die Verbindung wird an dem Anschluß aufgebaut, der als HTTP-Tunneling-Anschluß für den Besprechungsserver angegeben ist (standardmäßig 8081).

   Wenn der Client über einen HTTP-Proxy auf das Internet zugreifen muß und die Firewall des Clients abgehende Verbindungen nur über Anschluß 80 zuläßt, können Sie HTTP-Proxy-Tunneling über Anschluß 80 aktivieren. Weitere Informationen finden Sie unter Verbindung zum Besprechungsserver über Anschluß 80.

Verwandte Themen anzeigen
Meeting Services Netzwerkeinstellungen

## Verbindungen von der Komponente "Anwendung gemeinsam nutzen" zum Besprechungsserver

Die Komponente "Anwendung gemeinsam nutzen" muß eine Verbindung zur Besprechungsserver-Komponente des Sametime Servers aufbauen, damit ein Benutzer eine Anwendung auf seinem lokalen Computer mit entfernten Teilnehmern einer Online-Besprechung gemeinsam nutzen kann.

Die Komponente "Anwendung gemeinsam nutzen" kann an zwei Stellen in Sametime gestartet werden:

- im Sametime Connect Client,
- über die Schaltfläche "Anwendung gemeinsam nutzen" im Client-Java-Applet.

Der Sametime Server unterstützt eine direkte TCP/IP-Verbindung von der Komponente "Anwendung gemeinsam nutzen" zum Besprechungsserver. Der Sametime Server bietet auch HTTP- und HTTPS-Proxy-Tunneling sowie SOCKS-Proxy-Unterstützung für die Verbindung von der Komponente "Anwendung gemeinsam nutzen".

Wenn der Benutzer über einen Proxy-Server auf das Internet zugreift, muß er die Komponente "Anwendung gemeinsam nutzen" konfigurieren, um einen der unterstützten Proxy-Typen für die Verbindung zum Besprechungsserver zu verwenden. Weitere Informationen zu diesen Einstellungen finden Sie unter Verbindungseinstellungen für die Komponente "Anwendung gemeinsam nutzen".

Die folgenden Szenarien erklären Verbindungen von der Komponente "Anwendung gemeinsam nutzen":

**Die Komponente "Anwendung gemeinsam nutzen" im Sametime Connect Client starten**

Der folgende Verbindungsprozeß findet statt, wenn die Komponente "Anwendung gemeinsam nutzen" im Sametime Connect Client gestartet wird, um eine nicht geplante Besprechung mit gemeinsam genutzter Anwendung durchzuführen.

1. Der Endbenutzer klickt mit der rechten Maustaste im Sametime Connect Client auf den Namen eines Benutzers und wählt "Anwendung gemeinsam nutzen".
2. Um eine Anwendung von Sametime Connect aus gemeinsam zu nutzen, muß eine Online-Besprechung auf dem Besprechungsserver angelegt werden. Eine Verbindung zum Besprechungsserver wird aufgebaut, um die Besprechung zu erstellen.

   Die Verbindung zum Besprechungsserver erfolgt an dem Anschluß, der in den Sametime Verbindungseinstellungen des Sametime Connect Clients als Anschluß für gemeinsam genutzte Anwendungen festgelegt ist.
3. Ein Web-Browser und die Komponente "Anwendung gemeinsam nutzen" werden auf dem lokalen Computer des Benutzers gestartet. Das Java-Applet für den Betrachter der gemeinsam genutzten Anwendung wird auf den Web-Browser heruntergeladen und baut die Verbindung zum Besprechungsserver auf.

4. Die Komponente "Anwendung gemeinsam nutzen" baut eine Verbindung zum Sametime Besprechungsserver auf, von dem das Java-Applet heruntergeladen wurde. Weitere Informationen zur Java-Applet-Verbindung finden Sie unter Java-Applet-Verbindungen zum Online-Besprechungsserver.

**Starten der Komponente "Anwendung gemeinsam nutzen" von einem Java-Applet aus**

Der folgende Verbindungsprozeß findet statt, wenn die Komponente "Anwendung gemeinsam nutzen" vom Java-Applet aus gestartet wird, das bei einer Online-Besprechung vom Sametime Server zum Client heruntergeladen wurde.

1. Der Endbenutzer klickt im Java-Applet auf die Schaltfläche "Anwendung gemeinsam nutzen", um die Komponente "Anwendung gemeinsam nutzen" auf seinem lokalen Computer zu starten.
2. Die Komponente "Anwendung gemeinsam nutzen" wird gestartet und baut eine Verbindung zum Sametime Server auf, von dem der Java-Client heruntergeladen wurde.

Der vom Sametime Server heruntergeladene Code enthält die Einstellungen des Serveranschlusses, die für eine direkte, eine HTTP-, eine HTTPS- oder eine SOCKS-Proxy-Verbindung erforderlich sind.

Der Benutzer muß die Komponente "Anwendung gemeinsam nutzen" konfigurieren, um über eine direkte Verbindung (Kein Proxy), einen HTTP-Proxy, einen HTTPS-Proxy oder einen SOCKS-Proxy eine Verbindung aufzubauen. Wenn der Benutzer z. B. über einen HTTPS-Proxy auf das Internet zugreifen will, muß er in den Verbindungsoptionen der Komponente "Anwendung gemeinsam nutzen" die Option "HTTPS-Proxy" als Proxy-Typ wählen.

Verwandte Themen anzeigen
Sametime Verbindungseinstellungen für den Sametime Connect Client
Meeting Services Netzwerkeinstellungen

## Verbindungseinstellungen für die Komponente "Anwendung gemeinsam nutzen"

Wenn ein Client über einen Proxy-Server auf den Besprechungsserver zugreift, muß der Benutzer eventuell die Verbindungseinstellungen des Clients "Anwendung gemeinsam nutzen" ändern. Sobald der Benutzer diese Einstellungen definiert hat, sind spätere Änderungen erst dann erforderlich, wenn sich die Proxy- oder Firewall-Konfiguration des Benutzers ändert.

Der Benutzer kann Verbindungseinstellungen über die Schaltfläche "Anschlußmöglichkeit" des Clients "Anwendung gemeinsam nutzen" ändern.

**Hinweis** Der Sametime Connect Client umfaßt ebenfalls Verbindungseinstellungen. Die Verbindungseinstellungen des Sametime Connect Clients und der Komponente "Anwendung gemeinsam nutzen" werden beide in der Sametime Connect Datei connect.ini im Verzeichnis C:\Program Files\Lotus\Sametime Client auf dem lokalen Computer des Benutzers gespeichert. Wenn der Benutzer die Verbindungsoptionen für einen dieser Clients festlegt, verwendet der andere automatisch dieselben Einstellungen. Weitere Informationen finden Sie unter Verbindungsoptionen für den Sametime Connect Client.

Verbindungseinstellungen für die Komponente "Anwendung gemeinsam nutzen":

- **Kein Proxy** - Wählen Sie diese Option, wenn der Internet-Zugriff nicht über einen Proxy-Server erfolgt. Wenn diese Option aktiviert ist, baut die Komponente "Anwendung gemeinsam nutzen" eine direkte TCP/IP-Verbindung zum Besprechungsserver auf. Der Besprechungsserver wartet auf diese direkte Verbindung an dem Anschluß, der in den Einstellungen "Netzwerk und Sicherheit" im Sametime Administrationswerkzeug für den Besprechungsserver angegeben wurde (standardmäßig 8081).

  Diese Verbindungsmethode erzielt die beste Leistung bei gemeinsam genutzten Anwendungen in einer Online-Besprechung.
- **HTTP-Proxy** - Wählen Sie diese Option, wenn der Internet-Zugriff über einen HTTP-Proxy erfolgt. Der Besprechungsserver wartet auf diese HTTP-Verbindung an dem Anschluß, der in den Einstellungen "Netzwerk und Sicherheit" im Sametime Administrationswerkzeug als "HTTP-Tunnel-Anschluß " angegeben wurde.

  Für diese Option muß der Benutzer den DNS-Namen oder die IP-Adresse des HTTP-Proxy-Servers sowie den Anschluß für den HTTP-Proxy-Server angeben.

  Bei der Verbindung über einen HTTP-Proxy-Server kann sich die Leistung für gemeinsam genutzte Anwendungen verringern.

- **HTTPS-Proxy** - Wählen Sie diese Option, wenn der Internet-Zugriff über einen HTTPS-Proxy erfolgt. Der Besprechungsserver wartet auf diese Verbindung an dem Anschluß, der in den Einstellungen "Netzwerk und Sicherheit" im Sametime Administrationswerkzeug als "HTTPS-Anschluß des Meeting Servers" angegeben wurde.

  Für diese Option muß der Benutzer den DNS-Namen oder die IP-Adresse des HTTPS-Proxy-Servers sowie den Anschluß für den HTTPS-Proxy-Server angeben.

  Bei der Verbindung über einen HTTPS-Proxy-Server kann sich die Leistung für gemeinsam genutzte Anwendungen verringern.

- **Socks4-Proxy** - Wählen Sie diese Option, wenn der Internet-Zugriff über einen SOCKS4-Proxy erfolgt. Der Besprechungsserver wartet auf diese Verbindung an dem Anschluß, der in den Netzwerkeinstellungen des Besprechungsservers als Anschluß für den Besprechungsserver angegeben wurde.

  Für diese Option muß der Benutzer den DNS-Namen oder die IP-Adresse des SOCKS4-Proxy-Servers sowie den Anschluß für den SOCKS4-Proxy-Server angeben.

- **Socks5-Proxy** - Wählen Sie diese Option, wenn der Internet-Zugriff über einen SOCKS5-Proxy erfolgt. Der Besprechungsserver wartet auf diese Verbindung an dem Anschluß, der in den Einstellungen "Netzwerk und Sicherheit" im Sametime Administrationswerkzeug als Anschluß für den Besprechungsserver angegeben wurde.

  Für diese Option muß der Benutzer den DNS-Namen oder die IP-Adresse des SOCKS5-Proxy-Servers, den Anschluß für den SOCKS5-Proxy-Server und seinen SOCKS-Benutzernamen sowie sein Kennwort angeben.

- **Ausnahmen: Proxy-Server nicht für Adressen verwenden, die beginnen mit:** - Dieses Feld ermöglicht der Komponente "Anwendung gemeinsam nutzen" eine direkte Verbindung zu angegebenen Servern. Die Komponente "Anwendung gemeinsam nutzen" verwendet für diese Server auch dann die direkte Verbindungsmethode, wenn ein Proxy-Typ in den Verbindungseinstellungen des Clients gewählt ist. Die direkte Verbindungsmethode erzielt eine höhere Leistung bei gemeinsam genutzten Anwendungen als jede Proxy-Verbindungsmethode.

  Geben Sie das DNS-Suffix oder ein IP-Adressen-Präfix der Server ein, für die die Proxy-Verbindungsmethoden zugunsten der direkten Verbindungsmethode umgangen werden. Um z. B. eine direkte Verbindung zu einem Server mit dem Namen server1.acme.com oder server2.acme.com aufzubauen, gibt der Benutzer "acme.com" (das DNS-Suffix) in das Feld "Ausnahmen" ein.

  Der Benutzer kann auch IP-Adressen in das Feld "Ausnahmen" eingeben. Verwenden Sie das folgende Format für die IP-Adressen: 192.111 oder 192.111.105. Verbindungen werden zu Servern aufgebaut, die mit den angegebenen IP-Adressen beginnen.

  Sowohl die Komponente "Anwendung gemeinsam nutzen" als auch der Sametime Connect Client beziehen ihre Verbindungseinstellungen aus der Datei connect.ini auf dem lokalen Computer des Benutzers. Das Feld "Ausnahmen" ermöglicht dem Sametime Client die Verbindung über einen Proxy und der Komponente "Anwendung gemeinsam nutzen" das Umgehen des Proxy-Servers, um die Leistung für gemeinsam genutzte Anwendungen zu verbessern.

Verwandte Themen anzeigen
Meeting Services Netzwerkeinstellungen
Verbindung zum Sametime Besprechungsserver
Sametime Verbindungseinstellungen für den Sametime Connect Client

## Meeting Services Netzwerkeinstellungen

Der Besprechungsserver umfaßt die folgenden Netzwerkanschluß- und Tunneling-Einstellungen. Um auf diese Einstellungen zuzugreifen, öffnen Sie das Sametime Administrationswerkzeug, wählen Sie "Server" und dann "Netzwerk und Sicherheit". Diese Einstellungen befinden sich im Bereich "Netzwerkeinstellungen für Meeting Services" der Administrationsseite "Netzwerk und Sicherheit".

**Anschluß des Besprechungsservers**
Der Anschluß des Besprechungsservers wartet auf direkte TCP/IP-Verbindungen von den Client-Java-Applets (Betrachter für gemeinsam genutzte Anwendungen und Pinwand) und der OCX-Komponente "Anwendung gemeinsam nutzen". Der Standardanschluß für den Besprechungsserver ist Anschluß 8081.

Die OCX-Komponente "Anwendung gemeinsam nutzen" versucht eine direkte Verbindung zum Besprechungsserver am Anschluß für den Besprechungsserver, wenn der Benutzer in den Verbindungseinstellungen der Komponente "Anwendung gemeinsam nutzen" die Option "Kein Proxy" wählt.

Wenn Sie die Anschlußnummer ändern, müssen Clients, die nicht über einen Proxy-Server auf das Internet zugreifen, den Anschluß ändern, der in den Verbindungseinstellungen des Sametime Connect Clients als Anschluß für gemeinsam genutzte Anwendungen angegeben ist. Für diese Clients muß der Anschluß für gemeinsam genutzte Anwendungen im Sametime Connect Client mit dem Anschluß für den Besprechungsserver am Server übereinstimmen.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**Server-Kommunikationsanschluß T.120**
Der Server-Kommunikationsanschluß T.120 unterstützt T.120-Protokollverbindungen von anderen Sametime Servern und von Microsoft NetMeeting Clients. Die Standardeinstellung ist Anschluß 1503, der registrierte Anschluß für T.120-Verbindungen.

Ein Sametime Server baut eine Verbindung zu einem anderen Sametime Server auf, wenn ein Benutzer eine neue Besprechung anlegt und im Formular "Neue Besprechung" eine der folgenden Optionen wählt: "Teilnehmer können von Servern innerhalb des Unternehemens teilnehmen" oder "Teilnehmer aus dem Internet können teilnehmen".

Wenn eine dieser Optionen gewählt ist, verbindet der Sametime Server andere Sametime Server mit der Besprechung, sofern der Administrator die Verbindung der Server gestattet. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server.

Wenn zwei Sametime Server bei einer Online-Besprechung verbunden sind, werden alle Daten der Online-Besprechung zwischen dem Ausgangsserver und dem verbundenen Server über den Server-Kommunikationsanschluß T.120 übertragen.

Microsoft NetMeeting Clients bauen eine Verbindung zum Server ebenfalls über den T.120-Anschluß auf, wenn sie an Besprechungen teilnehmen, für die NetMeeting der angegebene Client ist. Ein Besprechungsverwalter kann beim Einrichten einer neuen Online-Besprechung NetMeeting als Client festlegen.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**HTTPS-Anschluß des Besprechungsservers**
Der HTTPS-Anschluß des Besprechungsservers wartet auf HTTPS-Verbindungen von der OCX-Komponente "Anwendung gemeinsam nutzen". Dieser Anschluß ermöglicht Clients der gemeinsamen Nutzung von Anwendungen, die über einen HTTPS-Proxy auf das Internet zugreifen, die Verbindung mit dem Besprechungsserver. Der HTTPS-Standardanschluß des Besprechungsservers HTTPS ist 8081.

Die Komponente "Anwendung gemeinsam nutzen" versucht am HTTPS-Anschluß des Besprechungsservers eine HTTPS-Verbindung zum Besprechungsserver, wenn der Benutzer die Option "HTTPS-Proxy" unter den Verbindungseinstellungen der Komponente "Anwendung gemeinsam nutzen" gewählt hat.

Wenn Sie diese Anschlußnummer ändern, müssen auch Sametime Connect Clients, die über einen HTTPS-Proxy-Server auf das Internet zugreifen, den Anschluß ändern, der unter den Verbindungseinstellungen des Sametime Connect Clients als Anschluß für gemeinsam genutzte Anwendungen angegeben ist. Für diese Clients muß der Anschluß für gemeinsam genutzte Anwendungen im Sametime Connect Client mit dem HTTPS-Anschluß für den Besprechungsserver am Server übereinstimmen.

Über den HTTPS-Anschluß des Besprechungsservers übertragene Daten werden nicht verschlüsselt. Um Besprechungsdaten zu verschlüsseln, muß der Besprechungsverwalter die Option zur Verschlüsselung der Besprechungsdaten im Bereich "Sicherheit" des Formulars "Neue Besprechung" aktivieren, wenn er eine neue Besprechung einrichtet.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**HTTP-Tunneling-Anschluß**
Der HTTP-Anschluß des Besprechungsservers wartet auf HTTP-Verbindungen vom Client-Java-Applet (Betrachter für gemeinsam genutzte Anwendungen und Pinwand) und der OCX-Komponente "Anwendung gemeinsam nutzen". Dieser Anschluß ermöglicht Clients, die über einen HTTP-Proxy auf das Internet zugreifen, eine Verbindung zum Besprechungsserver aufzubauen. Der HTTP-Tunneling-Anschluß des Besprechungsservers ist standardmäßig 8081.

Das Client-Java-Applet versucht automatisch eine HTTP-Proxy-Serververbindung, wenn der anfängliche Versuch einer direkten Verbindung fehlschlägt. Weitere Informationen finden Sie unter Java-Applet-Verbindungen zum Online-Besprechungsserver.

Die Komponente "Anwendung gemeinsam nutzen" versucht am HTTP-Tunneling-Anschluß eine HTTP-Verbindung zum Besprechungsserver, wenn der Benutzer die Option "HTTP-Proxy" in den Verbindungseinstellungen der Komponente "Anwendung gemeinsam nutzen" wählt.

Wenn Sie diese Anschlußnummer ändern, müssen auch Sametime Connect Clients, die über einen HTTP-Proxy auf das Internet zugreifen, den Anschluß ändern, der unter den Verbindungseinstellungen des Sametime Connect Clients als Anschluß für gemeinsam genutzte Anwendungen angegeben ist. Für diese Clients muß der Anschluß für gemeinsam genutzte Anwendungen in Sametime Connect Client mit dem HTTP-Tunneling-Anschluß am Server übereinstimmen.

Wenn Sie diese Einstellung ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderungen wirksam werden.

**An Host-Name binden**
Diese Option wird verwendet, um die IP-Adresse oder den Hostnamen, der im Feld "Hostname" angegeben ist, an die Komponente "Meeting Services" des Sametime Servers zu binden.

**Host-Name**
Das Feld "Host-Name" ermöglicht Ihnen, der Sametime Komponente "Meeting Services" eine IP-Adresse oder einen Hostnamen zuzuweisen. Wenn diese Option ein IP-Adresse enthält und das Feld "An Host-Name binden" auf "Ja" eingestellt ist, können Anfragen direkt über den für den Besprechungsserver angegebenen Anschluß an die Komponente "Meeting Services" des Sametime Servers gesendet werden.

Verwandte Themen anzeigen

- Java-Applet-Verbindungen zum Besprechungsserver
- Verbindungen von der Komponente "Anwendung gemeinsam nutzen" zum Besprechungsserver
- Sametime Verbindungseinstellungen für den Sametime Connect Client
- Verbindung zum Besprechungsserver über Anschluß 80

## Verbindung zum Besprechungsserver über Anschluß 80

Einige Clients besitzen Firewall-Konfigurationen, die abgehende Verbindungen nur an Anschluß 80 zulassen. Sie können dem Client-Java-Applet und der Komponente "Anwendung gemeinsam nutzen" die Verbindung zum Besprechungsserver über Anschluß 80 erlauben.

Um Verbindungen zum Besprechungsserver über Anschluß 80 zu ermöglichen, verwenden Sie das Feld "Host-Name" im Bereich "Meeting Services Netzwerk" der Administrationsseite "Netzwerk und Sicherheit" und weisen Sie der Komponente "Besprechungsserver" des Sametime Servers eine IP-Adresse zu. Binden Sie diese IP-Adresse mit Hilfe der Option "An Host-Name binden" an die Komponente "Besprechungsserver" des Sametime Servers. Setzen Sie im Bereich "Meeting Services Netzwerk" der Administrationsseite "Netzwerk und Sicherheit" den Besprechungsserver-Anschluß, den HTTPS-Anschluß des Besprechungsservers und den HTTP-Tunneling-Anschluß auf Anschluß 80. Diese Kombination von Einstellungen ermöglicht dem Besprechungsserver, an Anschluß 80 auf eine direkte, eine HTTPS- und eine HTTP-Verbindung zu warten.

Der Sametime HTTP-Server wartet ebenfalls an Anschluß 80 auf HTTP-Verbindungen. Da zwei Komponenten des Sametime Servers auf HTTP-Anfragen an Anschluß 80 warten, müssen Sie dem HTTP-Server auch einen Hostnamen zuweisen. Wenn Sie dem Sametime HTTP-Server und dem Sametime Besprechungsserver eine unterschiedliche IP-Adresse zuweisen, können beide an Anschluß 80 auf HTTP-Anfragen warten.

So ermöglichen Sie Verbindungen zum Besprechungsserver über Anschluß 80:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Name und Kennwort des Administrators ein, um das Sametime Administrationswerkzeug zu öffnen. Das Sametime Administrationswerkzeug zeigt die Administrationsseite "Netzwerk und Sicherheit" an.
3. Treffen Sie im Bereich "Meeting Services Netzwerk" der Administrationsseite "Netzwerk und Sicherheit" die folgenden Einstellungen:
   - Setzen Sie den Besprechungsserver-Anschluß auf 80.
   - Setzen Sie den HTTPS-Anschluß des Besprechungsservers auf 80.
   - Setzen Sie den HTTP-Tunneling-Anschluß auf 80.
   - Geben Sie in das Feld "Host -Name" eine IP-Adresse für den Besprechungsserver ein.
   - Wählen Sie "Ja" im Feld "An Host-Name binden".
   - Klicken Sie auf die Schaltfläche "Aktualisieren".
4. Wählen Sie im Menü des Sametime Administrationswerkzeugs "Server" und dann noch einmal "Server". Wählen Sie den Sametime Server, für den Sie Besprechungsserver-Verbindungen über Anschluß 80 erlauben wollen. Wählen Sie "Server bearbeiten".
5. Blättern Sie zum Abschnitt "HTTP-Server" des Serverdokuments.
6. Geben Sie in das Feld "Host-Name" des Abschnitts "HTTP-Server" eine IP-Adresse (oder einen DNS-Hostnamen) für den Sametime HTTP-Server ein.
7. Wählen Sie im Feld "An Host-Name binden" des Abschnitts "HTTP-Server" die Option Aktiviert".
8. Klicken Sie am oberen Rand des Serverdokuments auf die Schaltfläche "Speichern und Schließen".
9. Starten Sie den Server neu, damit die Änderungen wirksam werden.

**Hinweis** Wenn Sie Verbindungen zum Besprechungsserver über Anschluß 80 erlauben, sollten Benutzer von Sametime Connect Client auch den Anschluß für gemeinsam genutzte Anwendungen in den Verbindungseinstellungen von Sametime Connect Client auf Anschluß 80 ändern.

Verwandte Themen anzeigen
Meeting Services Netzwerkeinstellungen
Vom Sametime Server verwendete Anschlüsse

# Kapitel 05: Verwalten der Community Services

## Community Services Administrationseinstelllungen

Community Services unterstützen sämtliche Funktionen für Online-Awareness, sofortige Nachrichten und Chat, die mit dem Sametime Server verfügbar sind. Diese Funktionen gibt es im Sametime Connect Client und in den Funktionen "Wer ist online" und "Wer ist anwesend" von Datenbanken, die aus Sametime-aktivierten Schablonen erstellt wurden, z. B. aus der Diskussionsschablone (STDISCUSS.NTF). Die Funktionen "Wer ist online" und "Wer ist anwesend" können auch über Programmiertools des Sametime Toolkits in bestehende Notes Datenbanken integriert werden.

Sie können über das Sametime Administrationswerkzeug auf die Community Services Administrationseinstellungen zugreifen, indem Sie "Server" und dann "Community Services" wählen.

Mit Hilfe der Community Services Administrationseinstellungen können Sie:

- die Anzahl der Einträge auf jeder Seite im Dialogfeld "Zur Connect Liste hinzufügen" steuern.
- das Zeitintervall steuern, das zwischen Hinzufügen eines neuen Benutzers in das Sametime Adreßbuch und seinem Erscheinen im Sametime Connect Client und in den Listen "Wer ist online" und "Wer ist anwesend" verstreicht.
- die Häufigkeit von Server-Aktualisierungen vom Öffentlichen Adreßbuch zur Sametime Community steuern.
- die maximale Anzahl an Benutzer- und Server-Verbindungen zu den Sametime Servern steuern.

Das Sametime Administrationswerkzeug gestattet Ihnen auch, an alle bei den Community Services angemeldeten Benutzer eine Nachricht zu senden.

Informationen über Anschlüsse und Netzwerkeinstellungen für Community Services finden Sie unter Community Services Netzwerkeinstellungen.

Verwandte Themen anzeigen

Community Services
Sametime Connect
Community Services Netzwerkeinstellungen
Das Community Server Überwachungswerkzeug
Sametime Protokoll
Sametime-aktivierte Schablonen und Anwendungen

## Anzahl der Einträge auf jeder Seite im Dialogfeld "Zur Connect Liste hinzufügen"

Beim Hinzufügen von Personen oder Gruppen zum Sametime Connect Client kann ein Benutzer einzelne Namen oder Gruppen aus dem Adreßbuch wählen. Die Liste der Namen und Gruppen im Adreßbuch erscheinen auf einer Seite im Dialogfeld "Zur Connect Liste hinzufügen". Das Sametime Administrationswerkzeug umfaßt eine Einstellung, über die der Administrator die Anzahl der Einträge auf jeder Seite steuern kann. Standardmäßig erscheinen pro Seite 60 Einträge, das Minimum beträgt 5 Einträge und das Maximum 1440 Einträge. Lotus empfiehlt eine Einstellung zwischen 100 und 200 Einträgen.

**Hinweis** Um eine Seite im Dialogfeld "Zur Connect Liste hinzufügen" zu sehen, öffnen Sie Sametime Connect und klicken Sie auf "Hinzufügen". Klicken Sie auf die Schaltfläche "Adreßbuch" im Dialogfeld "Teilnehmer hinzufügen" oder "Gruppe hinzufügen". Das Dialogfeld "Zur Connect Liste hinzufügen" wird geöffnet. Alle Benutzer und Gruppen im Adreßbuch werden in "Zur Connect Liste hinzufügen" aufgeführt.

So ändern Sie die Anzahl der Einträge, die pro Seite im Dialogfeld "Zur Connect Liste hinzufügen" erscheinen:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Community Services".
2. Geben Sie in das Dialogfeld "Zur Connect Liste hinzufügen" die gewünschte Anzahl der Einträge pro Seite ein.
3. Klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung wirksam wird.

### Häufigkeit der Aktualisierung vom Öffentlichen Adreßbuch zur Sametime Community

Der Sametime Community Server erhält eine Liste von Benutzern aus dem Sametime Adreßbuch. Der Administrator kann steuern, wie häufig (in Minuten) der Community Server eine aktualisierte Liste von Benutzern aus dem Sametime Adreßbuch erhält. Diese Aktualisierung gewährleistet, daß kürzlich in das Sametime Adreßbuch aufgenommene Benutzer in Sametime Connect und den Listen "Wer ist online" und "Wer ist anwesend" erscheinen. Die Aktualisierung findet nur statt, wenn während des Aktualisierungsintervalls Änderungen im Adreßbuch erfolgt sind. Die Standardeinstellung ist 60 Minuten, das Minimum 5 Minuten und das Maximum 1440 Minuten.

So ändern Sie die Aktualisierungshäufigkeit vom Öffentlichen Adreßbuch zur Sametime Community:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Community Services".
2. Geben Sie in das Feld "Häufigkeit von Server-Aktualisierungen vom Öffentlichen Adreßbuch zur Sametime Community" einen neuen Wert für das Zeitintervall (in Minuten) ein, in dem Aktualisierungen erfolgen.
3. Klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung wirksam wird.

### Häufigkeit von Server-Aktualisierungen vom Öffentlichen Adreßbuch zur Sametime Community

Wenn Sie mehrere Sametime Server installiert haben, muß Community Services auf jedem Sametime Server über eine Liste aller anderen Sametime Server in der Sametime Community verfügen. Community Services stellt anhand dieser Liste sicher, daß Benutzer mit unterschiedlichen lokalen Sametime Servern untereinander Funktionen für Online-Awareness, sofortige Nachrichten und Chats verwenden können. Weitere Informationen über lokale Sametime Server finden Sie unter Verteilen von Benutzern auf mehrere Sametime Server.

Jeder Sametime Server besitzt ein Serverdokument im Adreßbuch. Jedes Sametime Serverdokument umfaßt den Datensatz "Ist das ein Sametime Server?", der den Server als Sametime Server identifiziert. Community Services erstellt anhand dieser Dokumente eine Liste der Sametime Server in der Domäne (oder Community). Das Sametime Administrationswerkzeug umfaßt eine Einstellung, mit deren Hilfe der Administrator das Zeitintervall steuern kann, in dem der Community Server eine aktualisierte Liste aller Sametime Server aus dem Öffentlichen Adreßbuch erhält. Die Standardeinstellung ist 60 Minuten, das Minimum 5 Minuten und das Maximum 1440 Minuten.

So ändern Sie die Häufigkeit von Server-Aktualisierungen vom Öffentlichen Adreßbuch zur Sametime Community:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Community Services".
2. Geben Sie in das Feld "Häufigkeit von Server-Aktualisierungen vom Öffentlichen Adreßbuch zur Sametime Community" das Zeitintervall in Minuten ein, in dem Aktualisierungen erfolgen sollen.
3. Klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung wirksam wird.

### Maximale Benutzer- und Serververbindungen zum Sametime Server

Der Administrator kann die maximal zulässige Anzahl an Verbindungen zu Community Services festlegen. Die Verbindungen umfassen sowohl Benutzer- (oder Client-) als auch Server-zu-Server-Verbindungen.

Eine Benutzer- (oder Client-) Verbindung findet statt, wenn sich ein Benutzer bei Sametime Connect anmeldet oder in einer Datenbank mit der Funktionalität "Wer ist anwesend" und "Wer ist online" präsent ist. Die Untergrenze sind 50 Verbindungen, die Obergrenze 20000. Verwenden Sie die Obergrenze nur für Server mit besten Verarbeitungsfähigkeiten, mindestens 512 MB RAM, eine 1 MB-Netzwerkkarte und Doppelprozessoren. In der Regel sind 8000 TCP/IP-Verbindungen für Computer empfohlen, die die System-Mindestanforderungen erfüllen.

Server-zu-Server-Verbindungen finden statt, wenn mehrere Sametime Server in einer Domino Umgebung instalilert sind und für Benutzer unterschiedliche lokale Server festgelegt sind. Wenn Benutzer unterschiedliche lokale Server verwenden, können zwei Benutzer an zwei unterschiedlichen Sametime Servern mit Community Services verbunden sein. Eine Server-zu-Server-Verbindung muß aufgebaut werden, damit diese Benutzer einander "sehen" und Chats führen können.

So ändern Sie die maximalen Benutzer- und Serververbindungen zum Sametime Server:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Community Services".
2. Geben Sie im Feld "Maximale Anzahl der Benutzer- und Verver-Verbindungen zum Sametime Server" die maximal zulässige Anzahl an Verbindungen zum Community Server an.
3. Klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung wirksam wird.

# Kapitel 06: Senden von Nachrichten

## Senden von Nachrichten

Verwenden Sie das Sametime Administrationswerkzeug, um eine Nachricht an alle Benutzer zu senden, die gerade bei Community Services angemeldet sind. Ein Benutzer ist bei Community Services angemeldet, wenn er:

- sich beim Sametime Connect Client anmeldet.
- auf eine Sametime-aktivierte Datenbank oder ein Dokument zugreift, das die Funktionalität "Wer ist online" und "Wer ist anwesend" enthält.

**Hinweis** Laden Sie den Sametime Connect Client nicht auf den Sametime Servercomputer herunter und installieren Sie ihn nicht. Verwenden Sie für die Kommunikation mit Community Services Benutzern vom Servercomputer aus die Funktion "Rundsendungs-Nachrichten" des Sametime Administrationswerkzeugs.

### Senden einer Nachricht

So senden Sie eine Nachricht an alle Benutzer, die bei Community Services angemeldet sind:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Nachricht senden".
2. Geben Sie die Nachricht in das vorgesehene Textfeld ein.
3. Klicken Sie auf "Senden". Sie erhalten eine Bestätigung, daß die Nachricht gesendet wurde.

Verwandte Themen anzeigen
Senden einer Nachricht

# Kapitel 07: Verwalten der Meeting Services

## Meeting Services Administrationseinstellungen

Meeting Services unterstützen alle Online-Besprechungsaktivitäten auf dem Sametime Server. Online-Besprechungen können im Sametime Besprechungszentrum und vom Sametime Connect Client gestartet werden.

Sie greifen auf die Meeting Services Administrationseinstellungen zu, indem Sie im Sametime Administrationswerkzeug "Server" und dann "Meeting Services" wählen.

Mit Hilfe der Meeting Services Administrationseinstellungen können Sie:

- Automatisch Besprechungen über ihren geplanten Endzeitpunkt ausdehnen
- Namen aller Besprechungsteilnehmer nach Ende der Besprechung im Dokument "Besprechungsdetails" aufzeichnen
- Sametime Besprechungsserver verbinden

Informationen über Anschlüsse und Netzwerkeinstellungen für Meeting Services finden Sie unter Info über Sametime Anschlüsse und Netzwerkeinstellungen.

Verwandte Themen anzeigen
    Das Besprechungsserver-Überwachungswerkzeug
    Meeting Services

## Automatische Verlängerung von Online-Besprechungen

Beim Einrichten einer Besprechung im Sametime Online-Besprechungszentrum legt der Besprechungsverwalter einen Zeitpunkt für das Ende der Besprechung fest. Mit Hilfe der Funktion "Online-Besprechungen automatisch verlängern" lassen sich alle Online-Besprechungen über ihren geplanten Endzeitpunkt ausdehnen, wenn zu diesem Zeitpunkt noch Teilnehmer vorhanden sind.

Sie können die Anzahl an Minuten festlegen, um die sich Online-Besprechungen verlängern sollen, wenn am geplanten Endzeitpunkt noch Teilnehmer vorhanden sind. Diese Funktion wird standardmäßig bei Installation und Setup von Sametime aktiviert.

Wenn Sie die Funktion "Besprechungen automatisch verlängern" ausschalten, enden alle Besprechungen an ihrem geplanten Endzeitpunkt, selbst wenn noch Teilnehmer anwesend sind. Alle Besprechungsteilnehmer erhalten in diesem Fall ca. drei Minuten vor Besprechungsende eine Warnmeldung. Schalten Sie diese Funktion aus, wenn ständig eine große Zahl aktiver Besprechungen die Serverleistung beeinträchtigt.

So verwenden Sie die Funktion "Besprechungen automatisch verlängern":

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Meeting Services".
   - **Damit Besprechungen über ihren geplanten Endzeitpunkt hinaus fortfahren**, markieren Sie das Feld "Automatisch über geplante Zeit hinaus verlängern, wenn noch Teilnehmer anwesend sind".

     Geben Sie im Feld "Besprechungsverlängerung um (Minuten)" die Anzahl an Minuten ein, um die sich die Besprechungen über den geplanten Endzeitpunkt hinaus verlängern sollen.
   - **Damit alle Besprechungen an ihrem geplanten Endzeitpunkt enden**, entfernen Sie die Markierung aus dem Feld "Automatisch über geplante Zeit hinaus verlängern, wenn noch Teilnehmer anwesend sind". Alle Teilnehmer erhalten etwa drei Minuten vor dem geplanten Besprechungsende eine entsprechende Warnmeldung.
2. Klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Server neu, damit die Änderung wirksam wird.

Verwandte Themen anzeigen
    Meeting Services Administrationseinstellungen

## Aufzeichnen der Namen von Besprechungsteilnehmern im Dokument "Besprechungsdetails"

Wenn eine Besprechung endet, wird das Dokument "Besprechungsdetails" für die Besprechung im Online-Besprechungszentrum gespeichert. Sie können diese Dokumente für beendete Besprechungen ansehen, indem Sie das Besprechungszentrum öffnen, die Ansicht "Beendet" wählen und auf den Besprechungsnamen klicken.

Das Sametime Administrationswerkzeug umfaßt eine Funktion, die es gestattet, alle Besprechungsteilnehmer am Ende einer Besprechung im Dokument "Besprechungsdetails" aufzuzeichnen. Diese Funktion ist nützlich, wenn Sie nach Ende einer Besprechung mit den Teilnehmern Kontakt aufnehmen wollen oder wenn Sie feststellen wollen, wer an einer bestimmten Besprechung teilgenommen hat. Diese Option wird standardmäßig bei Installation und Setup von Sametime ausgeschaltet.

So zeichnen Sie die Namen von Besprechungsteilnehmern nach Ende der Besprechung im Dokument "Besprechungsdetails" auf:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Name und Kennwort des Administrators ein.
3. Wählen Sie im Sametime Administrationswerkzeug "Servers" und dann "Meeting Services".
4. Markieren Sie das Feld "Noch der Besprechung Namen der Teilnehmer zum Besprechungsdokument hinzufügen".
5. Klicken Sie auf die Schaltfläche "Aktualisieren".
6. Starten Sie den Server neu, damit die Änderung wirksam wird.

Verwandte Themen anzeigen
Meeting Services Administrationseinstellungen

## Verbinden von Sametime Besprechungsservern

Wenn Sie mehrere Sametime Server installiert und als einzelne Community aktiviert haben, können Sie die Besprechungsserver verbinden.

Die Verbindung von Besprechungsservern bietet folgende Vorteile:

- Die Besprechungsserver-Leistung ist höher, auch wenn eine große Zahl von Sametime Benutzern vorhanden sind.
- Die Netzwerkauslastung wird optimiert.
- Internet-Clients können an Besprechungen teilnehmen, die auf einem Sametime Server innerhalb des Unternehmens-Firewalls stattfinden, ohne den Firewall zu überqueren.

Weitere Informationen finden Sie unter Verbinden von Besprechungsservern im Abschnitt "Arbeiten mit mehreren Sametime Servern" in der vorliegenden Dokumentation.

Verwandte Themen anzeigen
Verbinden von Besprechungsservern
Vorteile beim Verbinden mehrerer Online-Besprechungsserver
Verteilen von Belastung und Nutzung des Netzwerks
Firewalls und Sametime Internet-Server
Anlegen einer Besprechung auf verbundenen Servern
Erstellen von Verbindungsdokumenten für das Verbinden von Besprechungsservern
Bearbeiten und Löschen von Verbindungsdokumenten
Aktivieren mehrerer Sametime Server als eine einzige Community

# Kapitel 08: Überwachung und Protokollierung

## Sametime Überwachungs- und Protokollierungswerkzeuge

Mit Hilfe der Sametime Server Überwachungswerkzeuge können Sie Sametime Server Statistiken überwachen. Diese Überwachungswerkzeuge bieten sekundengenaue Information über Community Server und Meeting Server Aktivitäten, HTTP-Anforderungen und -Befehle sowie freien Speicherplatz auf dem Server. Die Monitore zeigen diese Information als grafische Balken- und Kreisdiagramme an.

Die Sametime Server Protokollierungswerkzeuge umfassen das Sametime Protokoll, das Notes Protokoll und das Web-Server-Protokoll. Das Sametime Protokoll zeichnet Community Services und Meeting Services Ereignisse in der Sametime Protokolldatenbank (STLog.nsf) auf. Sie können Community Services Ereignisse auch in einer Textdatei aufzeichnen. Sie können auch die Ereignisse festlegen, die im Sametime Protokoll aufgezeichnet werden sollen.

Das Notes Protokoll erfaßt Ereignisse, die sich auf Domino Application Services und Datenbanken auf dem Sametime Server beziehen. Das Web-Server-Protokoll zeichnet Informationen über HTTP-Anforderungen auf.

Verwandte Themen anzeigen
Überwachungswerkzeuge
Protokollierungswerkzeuge

## Überwachungswerkzeuge

Grafische Überwachungswerkzeuge bieten aktuelle Statistiken der Sametime Server Aktivität. So greifen Sie auf die Sametime Überwachungswerkzeuge zu:

1. Klicken Sie in der Seite "Willkommen bei Sametime" auf "Server-Administration".
2. Geben Sie Administratorname und -kennwort ein.
3. Wählen Sie "Überwachung" und wählen Sie dann eines der unten beschriebenen Überwachungswerkzeuge.

Nachstehende Tabelle beschreibt die grafischen Überwachungswerkzeuge.

| **Überwachungswerkzeug** | **Beschreibung** |
|---|---|
| Community Server | Verwendet Balkendiagramme für die Anzeige aktueller Information über die Anzahl aller Anmeldungen und aller eindeutiger Anmeldungen. |
| Besprechungsserver | Verwendet Balkendiagramme für die Anzeige aktueller Information über aktive Besprechungen, Besprechungsteilnehmer, Ablehnungen und Authentifizierungsfehler. |
| HTTP-Statistik | Verwendet Balkendiagramme für die Anzeige aktueller Information über HTTP-Anforderungen und -Befehle. |
| Speicherplatz | Verwendet ein Kreisdiagramm, um den freien Speicherplatz auf dem Server darzustellen. |

## Das Community Server Überwachungswerkzeug

Mit Hilfe des Community Server Überwachungswerkzeugs können Sie die Gesamtanzahl von Community Services Anmeldungen und die Gesamtanzahl von eindeutigen Anmeldungen überwachen. Das Überwachungswerkzeug bietet sekundengenaue Informationen über die Anmeldeaktivität in einem grafischen Balkendiagramm. Das Balkendiagramm wird in dem Zeitintervall aktualisiert, das Sie angeben.

So überwachen Sie Community Server Aktivitäten:

1. Öffnen Sie das Sametime Administrationswerkzeug.
2. Wählen Sie "Überwachung" und dann "Community Server".
3. Wählen Sie in der Dropdown-Liste "Wählen Sie eine Community Server Statistik" das Diagramm "Gesamtanzahl der Community Services Anmeldungen" oder "Gesamtanzahl der einzelnen Community Services Anmeldungen". Beide Diagramme werden nachstehend beschrieben.
4. Geben Sie ein Abrufintervall an. Das "Abfrageintervall" gibt das Zeitintervall (in Sekunden) an, in dem das gewählte Community Server Diagramm aktualisiert wird. Um das Intervall zu ändern, geben Sie einen anderen Wert in das Feld "Abfrageintervall" ein und klicken Sie auf die Schaltfläche "Aktualisieren".

**Gesamtanzahl von Community Services Anmeldungen**
Benutzer können sich vom Sametime Connect Client über die Funktionen "Wer ist anwesend" und "Wer ist online" einer Sametime-aktivierten Datenbank (z. B. einer Diskussionsdatenbank) bei den Community Services anmelden.

Dieses Balkendiagramm zeigt die Gesamtanzahl aller Anmeldungen bei den Community Services, einschließlich mehrerer Anmeldungen desselben Benutzers. Wenn derselbe Benutzer z. B. über den Sametime Connect Client und eine Sametime-aktivierte Datenbank angemeldet ist, zeigt das Diagramm zwei Anmeldungen für diesen Benutzer. Wenn Sie mehrere Sametime Server installiert und unterschiedliche lokale Sametime Server für die Mitglieder der Community festgelegt haben, kann ein anderer Server eine Verbindung zum Community Server aufbauen, um sicherzustellen, daß Benutzer mit unterschiedlichen lokalen Servern einander "sehen" und miteinander Chats halten können.

Dieses Diagramm wird im Abfrageintervall (in Sekunden) aktualisiert, das unter dem Diagramm angegeben ist. Bei jeder Aktualisierung bzw. in jedem Abfrageintervall erscheint ein neuer Balken links im Diagramm. Die Balken für ältere Statistiken verschieben sich nach rechts, wenn ein neuer Balken erscheint. Klicken Sie auf die Schaltfläche "Aktualisieren", um alle Balken außer dem neuesten aus dem Diagramm zu entfernen.

**Gesamtanzahl der einzelnen Community Services Anmeldungen**
Dieses Balkendiagramm zeigt die Gesamtanzahl aller eindeutigen Anmeldungen bei den Community Services. Wenn derselbe Benutzer über den Sametime Connect Client und eine Sametime-aktivierte Datenbank angemeldet ist, zeigt das Diagramm nur eine Anmeldung für diesen Benutzer. Sie können anhand dieses Diagramms die aktuelle Anzahl von Community Server Benutzern ermitteln.

Dieses Diagramm wird im Abfragenterval (in Sekunden) aktualisiert, das unter dem Diagramm angegeben ist. Bei jeder Aktualisierung bzw. in jedem Abfrageintervall erscheint ein neuer Balken links im Diagramm. Die Balken für ältere Statistiken verschieben sich nach rechts, wenn ein neuer Balken erscheint. Klicken Sie auf die Schaltfläche "Aktualisieren", um alle Balken außer dem neuesten aus dem Diagramm zu entfernen.

Verwandte Themen anzeigen
Community Services Administrationseinstelllungen
Überwachungswerkzeuge

## Das Besprechungsserver-Überwachungswerkzeug

Das Besprechungsserver-Überwachungswerkzeug bietet sekundengenaue Informationen über Meeting Services Aktivitäten. Diese Information wird in dem Zeitintervall aktualisiert, das Sie festlegen.

Aktivitäten des Besprechungsservers überwachen:

1. Öffnen Sie das Sametime Administrationswerkzeug.
2. Wählen Sie "Überwachung" und dann "Besprechungsserver".
3. Wählen Sie in der Dropdown-Liste "Wählen Sie eine Besprechungserver-Statistik" eines der verfügbaren Diagramme für die Besprechungsserverstatistik. Die Diagramme werden nachstehend beschrieben.
4. Geben Sie ein Zeitintervall an, in dem das gewählte Diagramm aktualisiert werden soll.

**Aktive Besprechungen**
Dieses Balkendiagramm zeigt die Gesamtanzahl aktiver Besprechungen (oder laufender Besprechungen) auf dem Sametime Server.

Sie können dieses Diagramm überwachen, um festzustellen, ob die Anzahl aktiver Besprechungen ständig hoch ist. Eine hohe Anzahl an aktiven Besprechungen deutet auf ein potentielles Leistungsproblem und kann aufzeigen, daß ein zusätzlicher Sametime Server benötigt wird. Weitere Informationen finden Sie unter Serverleistung und -wartung.

Dieses Diagramm wird im Abfrageintervall (in Sekunden) aktualisiert, das unter dem Diagramm angegeben ist. Bei jeder Aktualisierung bzw. in jedem Abfrageintervall erscheint ein neuer Balken links im Diagramm. Die Balken für ältere Statistiken verschieben sich nach rechts, wenn ein neuer Balken erscheint. Klicken Sie auf die Schaltfläche "Aktualisieren", um alle Balken außer dem neuesten aus dem Diagramm zu entfernen.

Um das Intervall zu ändern, ändern Sie den Wert im Feld "Abfrageintervall" ein und klicken Sie auf die Schaltfläche "Aktualisieren".

**Besprechungsserver-Verbindungen**
Dieses Balkendiagramm zeigt die Gesamtanzahl von Verbindungen zu den Meeting Services. Ein Benutzer ist mit den Meeting Services verbunden, wenn er an einer Besprechung im Sametime Online-Besprechungszentrum oder an einer nicht geplanten Besprechung mit gemeinsam genutzter Anwendung teilnimmt, die von Sametime Connect oder über die Funktion "Wer ist anwesend" oder "Wer ist online" einer Sametime-aktivierten Datenbank initiiert wurde. Andere Server bauen Verbindungen zu den Meeting Services auf, wenn Sie mehrere Besprechungsserver verbunden haben. Weitere Informationen finden Sie unter Verbinden von Besprechungsservern.

Sie können anhand dieses Diagramms ermitteln, ob die Anzahl der Verbindungen zum Besprechungsserver ständig hoch ist. Eine hohe Anzahl an Verbindungen zum Besprechungsserver deutet auf ein potentielles Leistungsproblem und kann aufzeigen, daß ein zusätzlicher Sametime Server benötigt wird.

Dieses Diagramm wird im Abfrageintervall (in Sekunden) aktualisiert, das unter dem Diagramm angegeben ist. Bei jeder Aktualisierung bzw. in jedem Abfrageintervall erscheint ein neuer Balken links im Diagramm. Die Balken für ältere Statistiken verschieben sich nach rechts, wenn ein neuer Balken erscheint. Klicken Sie auf die Schaltfläche "Aktualisieren", um alle Balken außer dem neuesten aus dem Diagramm zu entfernen.

Um das Intervall zu ändern, geben Sie einen anderen Wert in das Feld "Abfrageintervall" ein und klicken Sie auf die Schaltfläche "Aktualisieren".

**Besprechungen und Teilnehmer**
Dieses Balkendiagramm zeigt die Namen aktiver Besprechungen sowie die Anzahl der Teilnehmer an jeder Besprechung. Klicken Sie auf die Schaltfläche "Aktualisieren", um eine aktuelle Statistik zu erhalten. Das Balkendiagramm "Besprechungen und Teilnehmer" wird nur aktualisiert, wenn Sie auf die Schaltfläche "Aktualisieren" klicken.

Die Besprechungsnamen werden links neben dem Diagramm gezeigt. Die Anzahl der Teilnehmer wird entlang der Diagrammbasis angezeigt.

Anhand dieses Diagramms können Sie den Teilnahmeumfang an Besprechungen ermitteln. Viele aktive Besprechungen mit einer hohen Teilnehmerzahl deuten auf ein potentielles Leistungsproblem und können aufzeigen, daß ein zusätzlicher Sametime Server benötigt wird. Weitere Informationen finden Sie unter Serverleistung und -wartung.

Klicken Sie auf die Schaltfläche "Nach Teilnehmer sortieren", um die Besprechungen nach der Anzahl der Teilnehmer zu sortieren. Die Besprechung mit der höchsten Teilnehmerzahl erscheint am unteren Ende des Diagramms. Die Besprechung mit der geringsten Teilnehmerzahl erscheint am oberen Ende des Diagramms.

Klicken Sie auf die Schaltfläche "Nach Besprechungsnamen sortieren", um die Besprechungsnamen alphabetisch zu sortieren.

**Besprechungs- und Autentifizierungsfehler**
Dieses Balkendiagramm zeigt die Anzahl fehlgeschlagener Authentifizierungen für jede Besprechung. Ein Authentifizierungsfehler tritt auf, wenn ein Benutzer versucht, auf eine Besprechung zuzugreifen, aber aufgrund der Eingabe eines ungültigen Benutzernamens oder Kennworts abgewiesen wird. Klicken Sie auf die Schaltfläche "Aktualisieren", um eine aktuelle Statistik zu erhalten. Das Balkendiagramm "Besprechungs- und Autentifizierungsfehler" wird nur aktualisiert, wenn Sie auf die Schaltfläche "Aktualisieren" klicken.

Die Besprechungsnamen werden links neben dem Diagramm gezeigt. Die Anzahl der Authentifizierungsfehler wird entlang der Diagrammbasis angezeigt.

Klicken Sie auf die Schaltfläche "Nach Fehler sortieren", um die Besprechungen nach der Anzahl der Authentifizierungsfehler zu sortieren. Die Besprechung mit der höchsten Fehlerzahl erscheint am unteren Ende des Diagramms. Die Besprechung mit der geringsten Fehlerzahl erscheint am oberen Ende des Diagramms.

Klicken Sie auf die Schaltfläche "Nach Besprechungsnamen sortieren", um die Besprechungsnamen alphabetisch zu sortieren.

Verwandte Themen anzeigen

Meeting Services Administrationseinstellungen
Überwachungswerkzeuge

### HTTP-Statistik-Überwachungswerkzeug

Das HTTP-Statistik-Überwachungswerkzeug führt Buch über HTTP-Anforderungen und -Befehle.

So überwachen Sie HTTP-Statistiken:

1. Öffnen Sie das Sametime Administrationswerkzeug.
2. Wählen Sie "Überwachung" und dann "HTTP-Statistik".
3. Wählen Sie am unteren Rand des Diagramms "Domino HTTP-Anforderungen" oder "Domino HTTP-Befehle". Die Diagramme werden nachstehend beschrieben.

**Hinweis** Diese Diagramme werden automatisch alle 60 Sekunden aktualisiert.

**Domino HTTP-Anforderungen**
Wenn Sie "Domino HTTP-Anforderungen" wählen, erscheint ein Balkendiagramm mit Server-Anfragestatistiken für die aktuelle Serversitzung (der Zeitraum vom letzten Serverstart bis zum aktuellen Zeitpunkt). Eine Server-Anforderung tritt auf, wenn ein Benutzer oder ein anderer Server Ihren Server auffordert, eine Task auszuführen. Das Balkendiagramm zeigt den Durchschnitt und die Spitzen der Anforderungsanzahl pro Minute, pro 5 Minuten, pro Stunde und pro Tag. Es zeigt außerdem die Gesamtzahl aller Anforderungen in der aktuellen Sitzung.

Ermitteln Sie anhand dieses Diagramms, ob die Rate der Anforderungen an den Server steigt oder ob der Server eine konstante Spitzenbelastung erfährt. Steigende Serveranforderungen deuten auf ein potentielles Leistungsproblem und können aufzeigen, daß ein Server-Upgrade oder ein zusätzlicher Server benötigt wird.

**Domino HTTP-Befehle**
Wenn Sie am unteren Rand des Bildschirms auf "Domino HTTP-Befehle" klicken, zeigt das Sametime Administrationswerkzeug ein Balkendiagramm mit Server-Befehlsstatistiken für die aktuelle Serversitzung an. Analysieren Sie anhand dieser Information Typ und Anzahl der Aufgaben, die Ihr Server bewältigen muß, was Ihnen bei Überwachung und Verwaltung der Serverleistung helfen kann. Das Sametime Administrationswerkzeug zeigt Statistiken für HTTP-Befehle wie "OpenDatabase" und "EditDocument".

Verwandte Themen anzeigen
Der Abschnitt "HTTP" des Serverdokuments
Überwachungswerkzeuge

## Speicherplatz-Überwachungswerkzeug

So überwachen Sie den freien Speicherplatz auf dem Sametime Server:

1. Öffnen Sie das Sametime Administrationswerkzeug.
2. Wählen Sie "Überwachung" und dann "Speicherplatz".

   Das Sametime Administrationswerkzeug zeigt ein grafisches Kreisdiagramm für jede Festplatte des Servers an. Verwenden Sie diese Information, um Plattenspeicher freizugeben, bevor Benutzer Fehlermeldungen über Speichermangel erhalten, wenn sie versuchen, Daten auf dem Server zu speichern. Prüfen Sie anhand dieser Information auch den freien Speicherplatz, wenn Sie Protokollparameter für das Sametime Protokoll einstellen. Kürzere Protokollierungsintervalle können die Größe der Sametime Protokolldatenbank rapide erhöhen.

   Die Datenbank STCONF.NSF vergrößert sich auch je nach Anzahl von Besprechungen, die angelegt wurden. Sie können diese Datenbank häufig archivieren, damit sie nicht zu umfangreich wird.

   Der Web-Server speichert Bilddateien und Dateianlagen in einem Dateicache, um die Server-Reaktionszeit zu optimieren. Um die Größe dieses Caches zu kontrollieren, geben Sie Einstellungen für maximale Dateicache-Größe und "Aufräumen" an. Diese Einstellungen befinden sich im Abschnitt HTTP des Serverdokuments unter "Festplatten-Cache für Bilder und Dateien" .

Verwandte Themen anzeigen
Die Einstellungen "Festplatten-Cache für Bilder und Dateien" für den HTTP Server
Überwachungswerkzeuge

## Protokollierungswerkzeuge

Nachstehende Tabelle listet die Protokolle auf, die Daten über den Sametime Server aufzeichnen.

| Protokoll | Dateiname | Beschreibung |
|---|---|---|
| Sametime Protokoll | STLOG.NSF | Zeichnet Serveraktivitäten auf, die mit Meeting Services und Community Services zusammenhängen. |
| Notes Protokoll | LOG.NSF | Zeichnet Serveraktivitäten auf, die mit Domino Application Services zusammenhängen, z. B. Fehlermeldungen und Informationen über Benutzeraktivität, Datenbankaktivität und Netzwerkkommunikation. Enthält auch Informationen über Sametime Datenbanken. |
| Web-Server-Protokoll | DOMLOG.NSF | Zeichnet Informationen über HTTP-Anforderungen und -Befehle von Browsern auf. |

Verwandte Themen anzeigen
Sametime Protokoll
Festlegen der Protokollparameter für das Sametime Protokoll

## Sametime Protokoll

Die Sametime Protokolldatenbank (STLOG.NSF) zeichnet Serveraktivitäten im Zusammenhang mit Meeting Services und Community Services auf. Beim Setup wird die Sametime Protokolldatenbank automatisch angelegt, und der beim Setup angegebene Administrator erhält Manager-Zugriff auf die Zugriffskontrolliste (ACL) der Datenbank. Der Server erhält ebenfalls Manager-Zugriff auf die Datenbank, damit er Informationen in das Protokoll schreiben kann. Der Standardzugriff für alle anderen Benutzer ist "Leser".

Meeting Services und Community Services Ereignisse können in der Sametime Protokolldatenbank aufgezeichnet werden. Sie können das Sametime Protokoll auch so einrichten, daß Community Services Ereignisse in einer Textdatei protokolliert werden. Das Sametime Protokoll ist standardmäßig so eingestellt, daß Informationen in der Sametime Protokolldatenbank aufgezeichnet werden. Der Administrator kann wählen, welche Community Services und Meeting Services Ereignisse im Sametime Protokoll aufgezeichnet werden. Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.

Die Sametime Protokolldatenbank kann folgende Community Services und Meeting Services Ereignisse aufzeichnen:

- Datum und Uhrzeit von Anmeldungen und Abmeldungen bei Community Services
- Namen der Benutzer, die sich bei Community Services an- und abmelden
- Anwendungstyp (Web-Browser, Notes Client oder Sametime Connect), der für An- und Abmeldung bei Community Services verwendet wird
- Grund für gescheiterte Anmeldung bei Community Services
- IP-Adresse eines Community Services Benutzers
- Gesamtanzahl der Community Services Benutzer und Benutzeranmeldungen
- Status der Community Services Komponenten (gestartet oder gestoppt); Grund für Start- oder Stop-Ereignis sowie Name, IP-Adresse und Versionsnummer der Community Services Komponente
- Datum und Uhrzeit von Online-Besprechungsstarts
- Namen von Online-Besprechungen und Besprechungsverwaltern, die diese angelegt haben
- Anzahl der Teilnehmer
- Namen von Besprechungsteilnehmern und für jeden Teilnehmer der Zeitpunkt des Eintritts oder Verlassens der Besprechung
- Verschiedene Meeting Services Ereignisse, wie z. B. Starten und Stoppen einer Besprechung oder Hinzufügen und Entfernen eines Teilnehmers
- Kapazitätswarnungen, wenn die Auslastung der Meeting Services Parameter überschreitet, die der Administrator festgelegt hat

Verwandte Themen anzeigen
Festlegen der Protokollparameter für das Sametime Protokoll
Öffnen der Sametime Protokolldatenbank
Anzeigen der Sametime Protokolldatenbank

## Festlegen der Protokollparameter für das Sametime Protokoll

Beim Setup wird die Sametime Protokolldatenbank (STLOG.NSF) automatisch angelegt. Die Sametime Protokolldatenbank ist standardmäßig so eingestellt, daß sie Anmeldeaktivitäten der Community Services und allgemeine Meeting Services Ereignisse aufzeichnet.

Sie können das Sametime Protokoll so einstellen, daß es Meeting Services und Community Services Ereignisse in der Sametime Protokolldatenbank aufzeichnet, und die Community Services und Meeting Services Ereignisse angeben, die Sie im Protokoll wünschen. Sie können auch die Zeitspanne festlegen, nach der die in der Sametime Protokolldatenbank gesammelten Informationen auf dem Server gespeichert werden.

Community Services Ereignisse lassen sich in einer Textdatei protokollieren. Sie können die Protokolloptionen sowohl für die Datenbank als auch für die Textdatei aktivieren, wenn Sie die Information in der Sametime Protokolldatenbank und in einer Textdatei speichern wollen.

So richten Sie das Sametime Protokoll ein:

1. Öffnen Sie das Sametime Administrationswerkzeug.
2. Wählen Sie "Protokolle - Protokollparameter". Die Protokollparameter werden nachstehend beschrieben.
3. Wenn Sie einen der Protokollparameter ändern, klicken Sie auf die Schaltfläche "Aktualisieren" und starten Sie den Sametime Server neu, damit die Änderung wirksam wird.

Die folgenden Protokollparameter sind für das Sametime Protokoll verfügbar:

**Enable logging to a database (stlog.nsf)**
Wählen Sie diese Option, um Sametime Meeting Services und Community Services Daten in der Sametime Protokolldatenbank (STLog.nsf) zu speichern. Sie können auf die Sametime Protokolldatenbank zugreifen, indem Sie im Sametime Administrationswerkzeug "Protokolle - Sametime Protokoll" wählen. Diese Option ist standardmäßig ausgewählt.

**Enable logging to a text file**
Wählen Sie diese Option, um Community Services Daten in einer Textdatei zu speichern. Meeting Services Informationen erscheinen nicht in der Textprotokolldatei.

Wenn diese Option aktiviert ist, können Sie im Feld "Pfad und Dateiname für das Sametime Protokol" Speicherort und Namen der Textdatei angeben. Geben Sie z. B. C:\SAMETIMELOG\STLOG.TXT ein, um die Sametime Informationen in der Datei stlog.txt im Verzeichnis Sametimelog zu speichern. Die Textdatei wird standardmäßig SAMETIME.LOG genannt.

Wenn Sie Community Services Informationen in einer Textdatei protokollieren, müssen Sie in der Datei gespeicherte Informationen manuell auf der Server-Festplatte löschen.

**Protokoll entfernen nach (days)**
Sie müssen die Agents "dailyUsageSummary" und "purgeOldCommunityRecords" in der Datenbank STLOG.NSF aktivieren, bevor Sie diese Option verwenden können. Weitere Informationen finden Sie unter Details: Festlegen der Protokollparameter für das Sametime Protokoll.

Wenn die Agents aktiviert sind und Sie diese Option aktivieren, werden alte Informationen automatisch aus der Sametime Protokolldatenbank entfernt. Geben Sie im entsprechenden Feld das Alter der Information (in Tagen) ein, die automatisch aus der Datenbank entfernt werden soll.

Diese Einstellung entfernt keine Informationen, die in Textdateien gespeichert sind. Informationen in der Textdatei müssen Sie manuell löschen.

**Community Server events to log**
Wählen Sie die Community Services Ereignisse, die Sie in der Sametime Protokolldatenbank oder Textdatei wünschen.

**Erfolgreiche Anmeldungen** - Wählen Sie diese Option, um Informationen über erfolgreiche An- und Abmeldungen bei Community Services aufzuzeichnen. Die folgende Information wird protokolliert: Benutzername, Uhrzeit und Datum der An- oder Abmeldung, benutzter Anwendungstyp (Web-Browser, Notes Client oder Sametime Connect) für An- oder Abmeldung sowie die IP-Adresse des Computers des Benutzers. Diese Option ist standardmäßig aktiviert.

**Gescheiterte Anmeldungen** - Wählen Sie diese Option, um Informationen über gescheiterte Anmeldungen bei den Community Services aufzuzeichnen. Die folgende Information wird protokolliert: Benutzername, Uhrzeit und Datum der versuchten Anmeldung, benutzter Anwendungstyp (Web-Browser, Notes Client oder Sametime Connect) für die Anmeldung, die IP-Adresse des Computers des Benutzers und der Grund für die mißlungene Anmeldung.

**Total logins and total unique logins** - Wählen Sie diese Option, um Gesamtwerte über Anmeldungen bei Community Services aufzuzeichnen.

Benutzer können sich vom Sametime Connect Client und über die Funktionen "Wer ist anwesend" und "Wer ist online" einer Sametime-aktivierten Datenbank (z. B. einer Diskussionsdatenbank) bei den Community Services anmelden. Wenn ein Benutzer über Sametime Connect und eine Sametime-aktivierte Datenbank bei den Community Services angemeldet ist, werden zwei Anmeldungen in der Kategorie "Anmeldungen gesamt" aufgezeichnet.

Die Anzahl eindeutiger Anmeldungen gibt die Gesamtanzahl von Benutzern an, die zu einem gegebenen Zeitpunkt auf Community Services zugreifen. Wenn ein Benutzer über Sametime Connect und eine Sametime-aktivierte Datenbank bei den Community Services angemeldet ist, wird nur eine Anmeldung in der Kategorie "Anmeldungen gesamt" aufgezeichnet.

**Gesamtanzahl der Anmeldungen und einzelnen Anmeldunge (Minuten)** - Gibt das Zeitintervall (in Minuten) an, in dem die Statistiken über Gesamtzahl der Anmeldungen und eindeutige Anmeldungen in das Sametime Protokoll geschrieben werden. Wenn Sie ein kurzes Zeitintervall angeben, wie z. B. eine Minute, kann die Größe der Protokolldatenbank oder -Textdatei rapide wachsen. Prüfen Sie den verfügbaren Speicherplatz auf dem Server, bevor Sie ein kurzes Zeitintervall festlegen.

Sie können diese Statistik in der Ansicht "Community Server - Statistik - Gesamtauslastung" des Sametime Protokolls ansehen.

**Zu protokollierende Besprechungsserver-Ereignisse**
Wählen Sie die Ereignisse des Besprechungsservers, die Sie in der Sametime Protokolldatenbank aufzeichnen wollen. Diese Information erscheint nicht in der Sametime Protokoll-Textdatei.

**Allgemeine Meeting Services Ereignisse** - Wählen Sie diese Option, um die folgenden Informationen über jede Online-Besprechung aufzuzeichnen: Besprechungsname, Name des Besprechungsverwalters, Datum und Uhrzeit des Besprechungsbeginns, Anzahl der Teilnehmer, Namen der Teilnehmer und für jeden Teilnehmer der Zeitpunkt des Eintritts in oder Verlassens der Besprechung.

Sie können die Meeting Services Ereignisinformation in den Ansichten "Online-Besprechungsaktivität" und "Verschiedene Ereignisse" des Sametime Protokolls sehen.

**Kapazitätswarnungen**

Die Serverleistung kann sich verlangsamen, wenn viele Benutzer gleichzeitig auf den Server zugreifen oder wenn datenintensive Anwendungen oder Dateien in vielen Besprechungen gemeinsam benutzt werden. Mit Hilfe der Kapazitätswarnungen können Sie die Auslastung des Besprechungsservers überwachen und die Ursache geringer Serverleistung ermitteln. Wenn häufig eine große Benutzerzahl auf den Server zugreift oder viele Benutzer ständig datenintensive Anwendungen oder Dateien gemeinsam nutzen, müssen Sie evtl. einen zusätzlichen Sametime Server installieren. Weitere Informationen finden Sie unter Serverleistung und -wartung und Verwenden mehrerer Sametime Server.

**Anzahl der Teilnehmer in ALLEN aktiven Besprechungen überschritten** - Wählen Sie diese Option, um eine Kapazitätswarnung in das Sametime Protokoll zu schreiben, wenn die Anzahl der Teilnehmer in allen aktiven Besprechungen die angegebene Anzahl überschreitet. Die Standardeinstellung ist 500.

**Anzahl der aktiven Besprechungen überschritten** - Wählen Sie diese Option, um eine Kapazitätswarnung in das Sametime Protokoll zu schreiben, wenn die Anzahl der aktiven Besprechungen auf dem Server die angegebene Anzahl überschreitet. Die Standardeinstellung ist 100.

**Anzahl der Teilnehmer in einer aktiven Besprechung überschritten** - Wählen Sie diese Option, um eine Kapazitätswarnung in das Sametime Protokoll zu schreiben, wenn die Anzahl der Teilnehmer in einer aktiven Besprechung die angegebene Anzahl überschreitet. Die Standardeinstellung ist 50.

Verwandte Themen anzeigen

- Sametime Protokoll
- Öffnen der Sametime Protokolldatenbank
- Anzeigen der Sametime Protokolldatenbank
- Protokollierungswerkzeuge

## Details: Festlegen der Protokollparameter für das Sametime Protokoll

Die Einstellung "Protokoll löschen nach (Tagen)" hat nur eine Wirkung, wenn Sie die Agents "dailyUsageSummary" und "purgeOldCommunityRecords" in der Sametime Protokolldatenbank (STLOG.NSF) aktivieren. Ein Lotus Notes Client ist für die Aktivierung dieser Agents in STLOG.NSF erforderlich. Beim Aktivieren der Agents müssen Sie den Namen des Sametime Servers angeben, auf dem die Agents laufen werden.

Wenn Sie Sametime in einer reinen Web-Umgebung installiert haben und keine Notes Clients verwenden, können Sie die Sametime Community Services Information in einer Textdatei speichern. Sie können Informationen manuell aus der Textdatei löschen, wenn das Textprotokoll zu umfangreich wird. In der reinen Web-Umgebung können Sie auch die Meeting Services und Community Services Information in der Sametime Protokolldatenbank speichern. Sie können jedoch keine alte Information aus der Datenbank entfernen, ohne die Agents über einen Lotus Notes Client zu aktivieren.

## Öffnen der Sametime Protokolldatenbank

So öffnen Sie die Sametime Protokolldatenbank:

1. Wählen Sie im Sametime Administrationswerkzeug "Protokolle" und dann "Sametime Protokoll".
2. Wählen Sie eine Ansicht.

Verwandte Themen anzeigen
Sametime Protokoll
Protokollierungswerkzeuge

## Anzeigen der Sametime Protokolldatenbank

Nachstehende Tabelle beschreibt die Ansichten in der Sametime Protokolldatenbank und die Informationen, die verfügbar sind, wenn der Administrator alle Community Services und Meeting Services Ereignisse protokollieren läßt. Standardmäßig zeichnet das Sametime Protokoll Informationen über Anmeldeaktivitäten bei den Community Services sowie allgemeine Meeting Services Ereignisse auf.

Wählen Sie die Community Services und Meeting Services Ereignisse, die Sie aufzeichnen wollen, indem Sie im Sametime Administrationswerkzeug "Protokolle - Protokollparameter" wählen.

**Hinweis** Wenn Sie beim Zugriff auf eine Ansicht die Meldung "Keine Dokumente gefunden" erhalten, prüfen Sie die Einstellungen in den Protokollparametern des Sametime Protokolls. Die Protokollparameter können die Aufzeichnung bestimmter Informationen im Protokoll unterdrücken.

| Ansicht | Beschreibung |
|---|---|
| Community Server Aktivitäten - Ereignisse<br><br>- Nach Anwendung<br>- Fehlgeschlagene Anmeldungen nach Zeit<br>- Anmeldung/Abmeldung<br>- Nach Zeit<br>- Anmeldung/Abmeldung<br>- Nach Zeit | Die ersten vier Ansichten unter "Community Server Aktivitäten - Ereignisse", die in der Sametime Protokolldatenbank zur Verfügung stehen, bieten ähnliche Informationen über Benutzeran- und -abmeldungen bei den Community Services. Jede Ansicht enthält ganz oder teilweise die folgende Information nach unterschiedlichen Kriterien sortiert.<br>Die links aufgeführten vier Ansichten unter "Community Server Aktivitäten - Ereignisse" enthalten folgende Informationen:<br><br>**Anwendungstyp** - Typ der Anwendung, über die sich der Benutzer angemeldet hat (Sametime Connect, Web-Browser oder Notes Client).<br>**Zeit** - Datum und Uhrzeit der An- oder Abmeldung durch einen Benutzer.<br><br>**Ereignistyp** - Der Ereignistyp ist entweder "Anmeldung", "Abmeldung" oder "Fehlgeschlagene Anmeldung".<br><br>**Benutzer-ID** - Eine Lotus Notes Benutzer-ID (autorisierter Name) oder ein Benultzername (aus dem Personendokument des Benutzers).<br><br>**IP-Adresse** - IP-Adresse des Computers des Benutzers.<br><br>**Fehlerquelle** - Grund für die fehlgeschlagene Anmeldung. Gibt auch an, ob sich ein Benutzer normal abmelden konnte. |
| Community Server Aktivitäten - Ereignisse - Systemstatus | Diese Ansicht zeigt die folgenden Informationen über Starten und Stoppen von Community Services Komponenten auf:<br><br>**Tag** - Datum, an dem der Status der Community Service Komponente mitgeteilt wurde.<br><br>**Zeit** - Uhrzeit, an der das Ereignis stattfand.<br><br>**Komponente** - Name der Community Server Komponente, die gestartet oder gestoppt wurde.<br><br>**IP-Adresse** - IP-Adresse des Servers, auf dem die Community Services Komponente installiert ist.<br><br>**Version** - Versionsnummer der Community Services Komponente, die gestartet oder gestoppt wurde. Für Stop-Ereignisse ist dieses Feld leer.<br><br>**Ereignistyp** - Der Ereignistyp ist "Start" oder "Stop".<br><br>**Grund** - Grund für das Stoppen der Community Services Komponente. Für Start-Ereignisse ist dieses Feld leer. |

| | |
|---|---|
| Aktivitäten - Statistik - Tägliche Gesamtauslastung | Diese Ansicht zeigt die Gesamtanzahl aller Community Services Benutzer und Anmeldungen für jeden Tag. Die Gesamtanzahl der Benutzer kann sich von der Anzahl der Anmeldungen unterscheiden, da sich ein Benutzer von verschiedenen Standorten bei den Community Services anmelden kann (z. B. von Sametime Connect und von einer Sametime Diskussionsdatenbank). Diese Ansicht enthält die folgenden Informationen, nach Monat und Tag kategorisiert:<br><br>**Benutzer gesamt** - Gesamtzahl der Benutzer, die am gewählten Datum auf Community Services zugegriffen haben.<br><br>**Minimum** - Anzahl der Benutzer, die während der geringsten Serverbelastung auf Community Services zugegriffen haben.<br><br>**Maximum** - Anzahl der Benutzer, die während der höchsten Serverbelastung auf Community Services zugegriffen haben.<br><br>**Mittelwert** - Durchschnittliche Anzahl der Community Services Benutzer am gewählten Datum. |
| Community Server Aktivitäten - Statistik - Gesamtauslastung | Diese Ansicht bietet Informationen über die Gesamtanzahl der Community Services Benutzer und der Anmeldungen. Diese Information wird in dem Zeitintervall (in Minuten) angegeben, das Sie im Sametime Administrationswerkzeug bei den Protokollparametern festlegen. |
| Verschiedene Ereignisse | Diese Ansicht zeigt Meeting Services Ereignisse, wie z. B. Starten und Stoppen einer Besprechung und Hinzufügen und Entfernen von Teilnehmern. Für jedes Besprechungsereignis werden Datum und Uhrzeit, Ereignistyp, Besprechungs-Handle und Besprechungsname angegeben. Für jedes teilnehmerbezogene Ereignis werden Datum und Uhrzeit, Ereignistyp, Besprechungs-Handle und der Name des Teilnehmers angegeben. |

| | |
|---|---|
| Online Meeting Activity | Diese Ansicht zeigt die folgenden Informationen über jede Online-Besprechung. Sie können auch festlegen, daß Warnungen erscheinen, wenn die Anzahl aktiver Besprechungen und mit den Meeting Services verbundener Benutzer eine von Ihnen angegebene Grenze erreicht.<br>**Besprechungsname** - Name der Besprechung.<br>**Datum** - Datum des Besprechungsbeginns.<br>**Besprechungsverwalter** - Person, die die Besprechung angelegt hat.<br>**Zeit** - Uhrzeit des Besprechungsbeginns.<br>**Anzahl Teilnehmer** - Anzahl der Personen, die an der Besprechung teilgenommen haben.<br>**Teilnehmernamen** - Notes ID oder Benutzername jeder Person, die an der Besprechung teilgenommen hat. Anonyme Benutzer werden als "Anonym" aufgelistet. Um diese Information zu sehen, klicken Sie auf den Besprechungsnamen, wählen Sie "Datum" und klicken Sie auf den Namen des Besprechungsverwalters.<br>**Zeit teilgenommen/Zeit verlassen** - Uhrzeit, an der jeder Benutzer in die Besprechung eingetreten ist oder sie verlassen hat. Um diese Information zu sehen, klicken Sie auf den Besprechungsnamen, dann auf das Datum und den Namen des Besprechungsverwalters.<br>**Kapazitätswarnungen:** Anhand der folgenden drei Kapazitätswarnungen können Sie die Auslastung des Besprechungsservers überwachen und die Ursache geringer Serverleistung bestimmen.<br>● **Anzahl der Teilnehmer in ALLEN Besprechungen überschritten** - Die Anzahl aller Teilnehmer an allen aktiven Besprechungen hat die in den Sametime Protokollparametern festgelegte Anzahl überschritten. Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.<br>● **Anzahl der Teilnehmer in einer Besprechung überschritten** - Die Anzahl aller Teilnehmer an einer aktiven Besprechung hat die festgelegte Anzahl überschritten. Die Standardeinstellung ist 50. Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.<br>● **Anzahl der aktiven Besprechungen überschritten** - Die Anzahl aktiver Besprechungen hat die in den Sametime Protokollparametern festgelegte Anzahl überschritten. Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll. |

Verwandte Themen anzeigen

Sametime Protokoll
Protokollierungswerkzeuge

## Notes Protokoll

Die Notes Protokolldatenbank (LOG.NSF) zeichnet Server-Aktivitätsinformationen über Domino Application Services und Datenbanken auf dem Sametime Server auf. Beim Setup wird die Notes Protokolldatenbank (LOG.NSF) automatisch angelegt und der Server erhält Manager-Zugriff in der Zugriffskontrolliste (ACL) der Datenbank. Der Standardzugriff für alle Benutzer ist "Leser".

Die Notes Protokolldatenbank zeichnet Informationen über alle Serveraktivitäten auf, z. B. Datenbankgröße und -benutzer, Server-Ereignisse, Anrufe beim und vom Server und die Kostenerfassung für Serverdienste. Prüfen Sie das Notes Protokoll, um folgendes zu überwachen:

- Verfügbarer Speicherplatz auf dem Server
- Verfügbarer Server-Hauptspeicher
- Serverauslastung
- Serverleistung
- Datenbanken, die Wartung benötigen

Verwandte Themen anzeigen
- Öffnen der Notes Protokolldatenbank
- Anzeigen der Notes Protokolldatenbank
- Protokollierungswerkzeuge

## Öffnen der Notes Protokolldatenbank

So öffnen Sie die Notes Protokolldatenbank (LOG.NSF):

1. Wählen Sie im Sametime Administrationswerkzeug "Protokolle" und dann "Notes Protokoll".
2. Wählen Sie eine Ansicht.

Verwandte Themen anzeigen
- Notes Protokoll
- Protokollierungswerkzeuge

## Anzeigen der Notes Protokolldatenbank

Nachstehende Tabelle beschreibt die Ansichten in der Notes Protokolldatenbank (LOG.NSF).

| Ansicht | Beschreibung |
|---|---|
| Datenbank-Größe | Zeigt Größe und Auslastung aller Datenbanken auf dem Server. Diese Ansicht listet die Größe der Datenbank, den von der Datenbank benutzten Speicherplatz in Prozent und die wöchentliche Auslastung auf.<br>Ermitteln Sie anhand dieser Ansicht unbenutzte Ansichten, Datenbankgröße und unbenutzten Speicherplatz in der Datenbank. |
| Datenbank-Auslastung | Zeigt die Auslastung aller Datenbanken auf dem Server. Diese Ansicht listet Datum und Uhrzeit von Datenbankzugriffen auf, Art des Zugriffs und den Namen des zugreifenden Benutzers.<br>Ermitteln Sie anhand dieser Ansicht unbenutzte Ansichten, Datenbankgröße und unbenutzten Speicherplatz in einer Datenbank. |
| Mail-Routing-Ereignisse | Diese Ansicht wird vom Sametime Server nicht benutzt. |

| | |
|---|---|
| Verschiedene Ereignisse | Zeigt Sametime Ereignisse und Fehlermeldungen, die nicht in anderen Ansichten verfügbar sind. Meldungen werden in chronologischer Reihenfolge sortiert. Ermitteln Sie anhand dieser Ansicht Sametime Fehlermeldungen, Serverausfälle und beschädigte Datenbanken. |
| NNTP-Ereignisse | Diese Ansicht wird vom Sametime Server nicht benutzt. |
| Anrufe - Nach Datum | Diese Ansicht wird vom Sametime Server nicht benutzt. |
| Anrufe - Nach Benutzer | Diese Ansicht wird vom Sametime Server nicht benutzt. |
| Replizierungsereignisse | Diese Ansicht wird vom Sametime Server nicht benutzt. |
| Beispiel-Kostenerfassung | Zeigt dieselbe Information wie die Ansichten über Auslastung, jedoch sind die Informationen nicht kategorisiert. Die Informationen in dieser Ansicht lassen sich einfach in eine Tabellenkalkulation exportieren. Verwenden Sie diese Ansicht zur Kostenerfassung, z. B. für Nutzung des Bespechungszentrums, des Netzwerks und von Datenbanken. |
| Auslastung - Nach Datum | Zeigt Sametime Benutzertransaktionen nach Datum sortiert. Transaktionen sind Operationen wie Starten von oder Teilnehmen an Besprechungen, Öffnen von Dokumenten und Aktualisieren von Dokumenten. Jeder Datensatz listet Datum und Uhrzeit der Transaktion, Anzahl der Lese- und Schreib-Operationen, Größe der Datenbank und Gesamtanzahl der Transaktionen auf. Prüfen Sie anhand dieser Ansicht die Datenbankauslastung und Benutzertransaktionen mit dem Server an einem bestimmten Datum. |
| Auslastung - Nach Benutzer | Zeigt Sametime Benutzertransaktionen nach Benutzername. Transaktionen sind Operationen wie Starten von oder Teilnehmen an Besprechungen, Öffnen von Dokumenten und Aktualisieren von Dokumenten. Jeder Datensatz listet Benutzernamen, Datum und Uhrzeit der Transaktion, Anzahl der Lese- und Schreib-Operationen, Größe der Datenbank und Gesamtanzahl der Transaktionen auf. Prüfen Sie anhand dieser Ansicht die Transaktionen eines bestimmten Benutzers an einer Datenbank. |

Verwandte Themen anzeigen
Notes Protokoll
Protokollierungswerkzeuge

## Web-Server-Protokoll

Das Web-Server-Protokoll zeichnet Informationen über HTTP-Anforderungen von Browsern auf. Das Web-Server-Protokoll ist standardmäßig nicht aktiviert. Wenn Sie dieses Protokoll aktivieren, empfiehlt Lotus, daß Sie diese Informationen in den Web-Server-Protokolltextdateien speichern.

Sie können anhand der Web-Server-Protokollinformationen ermitteln, wie Web-Clients den Server nutzen. Mit jeder HTTP-Anforderung von einem Browser zeichnet der Sametime Server folgende Informationen auf:

- Datum und Uhrzeit der Anforderung
- IP-Adresse des Benutzers (oder die DNS-Adresse, wenn DNS Lookup im Serverdokument aktiviert ist)
- Name des Benutzers, wenn der Browser-Client über grundlegende Kennwortauthentifizierung oder Secure Sockets Layer- (SSL) Zertifizierung auf den Server zugegriffen hat
- Statuscode, den der Server an den Browser zurückgibt, um mitzuteilen, ob die Anforderung erfolgreich war
- Anzahl der Datenbytes, die vom Server an den Browser übertragen wurden
- Typ der Daten, z. B. Text oder Bild, auf die der Browser-Client zugegriffen hat

- HTTP-Anforderung, die vom Browser an den Server gesendet wurde
- Typ des Browsers, der für den Serverzugriff verwendet wurde
- Interne und CGI-Programmfehler
- Den referenzierenden URL, den der Browser für den Zugriff auf eine Seite dieser Site verwendet hat

Verwandte Themen anzeigen
Protokollierungswerkzeuge

## Web-Server-Protokoll-Textdateien

Sie können Web-Server-Informationen in Textdateien protokollieren, indem Sie das Feld "Protokolldateien" unter "Protokollierung aktivieren für" im Abschnitt "HTTP Server" des Serverdokuments aktivieren. Der Sametime Server beginnt jeden Tag eine neue Protokolldatei und fügt ihr mit jeder HTTP-Anforderung Daten hinzu. Der Sametime Server verwendet den Dateinamen, den Sie im Serverdokument angegeben haben, und fügt eine Datumserweiterung im Format *mmmttjj* hinzu, wobei *mmm* die ersten drei Buchstaben des Monats, *tt* den Tag des Monats und *jj* die letzten beiden Ziffern der Jahreszahl angibt. Beispielsweise bezeichnet agent_log.jul2196 das Datum 21. Juli 1996. Der Sametime Server legt um Mitternacht eine neue Protokolldatei an, wenn der Server läuft. Falls der Server nicht über Nacht läuft, erstellt er eine neue Protokolldatei, wenn Sie den Server am nächsten Tag starten.

Für eine geringere Belegung des Plattenspeichers sollten Sie regelmäßig die Größe der Protokolldateien prüfen, um sicherzustellen, daß sie nicht zu viel Speicherplatz beanspruchen, und die nicht mehr benötigten Protokolldateien löschen. Sie können auch über den Abschnitt "Vom Protokoll ausschließen" im Serverdokument bestimmte Arten der Protokollinformation ausschließen.

Nachstehende Tabelle listet die Information auf, die jede Protokolldatei aufzeichnet.

| **Name der Protokolldatei** | **Aufgezeichnete Informationen** |
|---|---|
| ACCESS-LOG | Zeichnet jedesmal die folgende Information auf, wenn ein Browser-Client eine Anforderung an den Server sendet:<br>● Datum und Uhrzeit der Anforderung<br>● IP-Adresse des Benutzers (oder die DNS-Adresse, wenn DNS-Suche im Serverdokument aktiviert ist)<br>● Name des Benutzers, wenn der Browser-Client über grundlegende Kennwortauthentifizierung auf den Server zugegriffen hat<br>● Statuscode, den der Server an den Browser zurückgibt, um mitzuteilen, ob die Anforderung erfolgreich war |
| AGENT-LOG | Zeichnet die folgenden Informationen auf:<br>● Datum und Uhrzeit der Anforderung<br>● Typ des Browsers, der für den Serverzugriff verwendet wurde<br>● Statuscode, den der Server an den Browser zurückgibt, um mitzuteilen, ob die Anforderung erfolgreich war |
| ERROR-LOG | Zeichnet interne Serverfehler auf |
| CGI-ERROR-LOG | Zeichnet Standardfehler (stderr) von CGI-Programmen auf |
| REFERER-LOG | Zeichnet die folgenden Informationen auf:<br>● Datum und Uhrzeit der Anforderung<br>● Referenzierenden URL, den der Browser-Client für den Zugriff auf eine Seite dieser Site verwendet hat<br>● Statuscode, den der Server an den Browser zurückgibt, um mitzuteilen, ob die Anforderung erfolgreich war |

Verwandte Themen anzeigen
Einrichten der Web-Server-Protokolldateien
Protokollierungswerkzeuge

## Einrichten der Web-Server-Protokolldateien

So richten Sie die Protokollierung von Web-Server-Informationen in Textdateien ein:

1. Klicken Sie im Sametime Administrationswerkzeugl auf "Server" und dann noch einmal auf "Server".
2. Wählen Sie das Serverdokument für den Server.
3. Klicken Sie auf "Server bearbeiten", um das Serverdokument in den Bearbeitungsmodus zu bringen.
4. Blättern Sie zum Abschnitt "HTTP Server".
5. Stellen Sie im Abschnitt "Protokollierung aktivieren für" das Feld "Protokolldateien" auf "Aktiviert" ein.
6. Führen Sie im Abschnitt "Protokolldatei-Einstellungen" folgende Aktionen durch:
   - Wählen Sie im Feld "Zugriffsprotokollformat" die Option "Allgemein", um nur Zugriffsinformationen oder wählen Sie "Erweitert allgemein", um Informationen über Zugriff, Agent und Referenzierung in der Zugriffsprotokolldatei aufzuzeichnen.
   - Wählen Sie im Feld "Zeitformat" die Option "Lokale Zeit", um Anforderungen in der Lokalzeit aufzuzeichnen, die auf Ihrem System eingestellt ist, oder wählen Sie "GMT", um Anforderungen in Greenwich Mean Time aufzuzeichnen.
7. Führen Sie im Abschnitt "Namen der Protokolldateien" folgende Aktionen durch:
   - Geben Sie einen Verzeichnisnamen in das Feld "Verzeichnis für Protokolldateien" ein, wenn Sie Protokolldateien in einem anderen als dem Sametime Datenverzeichnis speichern wollen.
   - Um andere als die vorgegebenen Namen für Protokolldateien zu verwenden, geben Sie einen Dateinamen in eines oder mehrere der folgenden Felder ein: Zugriffsprotokoll, Agent-Protokoll, Referenzprotokoll, Fehlerprotokoll, CGI-Fehlerprotokoll. Geben Sie keine Dateinamenerweiterung ein. Der Sametime Server hängt automatisch das Datum als Dateinamenerweiterung an.
8. Führen Sie im Abschnitt "Vom Protokoll ausschließen" eine oder mehrere der folgenden Aktionen aus, um Protokolleinträge für bestimmte Arten von Anforderungen auszuschließen:
   - Geben Sie eine auszuschließende URL-Adresse ein (z. B. *.gif).
   - Geben Sie auszuschließende HTTP-Methoden ein (z. B. POST oder DELETE).
   - Geben Sie auszuschließende MIME-Typen ein (z. B. image/gif).
   - Geben Sie auszuschließende Benutzer-Agenten ein (z. B. Mozilla).
   - Geben Sie auszuschließende Statuscodes ein (z. B. 300).
   - Geben Sie auszuschließende Hosts oder Domänen ein (z. B. 130.333.* oder *.edu).
9. Speichern Sie das Dokument.

   Verwandte Themen anzeigen
   
   Details: Einrichten der Web-Server-Protokolldateien
   Web-Server-Protokoll-Textdateien
   Protokollierungswerkzeuge

### Details: Einrichten der Web-Server-Protokolldateien

Wenn Sie die Protokollierung in Textdateien aktivieren und keine Namen für die Protokolldateien angeben, erstellt der Sametime Server die Protokolldateien mit ihren vorgegebenen Namen: ACCESS-LOG, AGENT-LOG, REFERER-LOG, ERROR-LOG und CGI-ERROR-LOG. Wenn Sie kein Verzeichnis für die Protokolldateien angeben, legt der Sametime Server diese Dateien im Sametime Datenverzeichnis an.

Um eine Schablone für den Hostnamen in das Feld "Auszuschließende Hosts und Domänen" einzugeben, müssen Sie die Einstellung "DNS-Suche" im Serverdokument aktivieren. Wenn diese Option deaktiviert ist, können Sie nur IP-Adreßschablonen verwenden. Wenn die Option "DNS-Suche" aktiviert ist, können Sie z. B. www.internotes.lotus.com; www.lotus.com; *.ibm.com verwenden. Andernfalls müssen Sie eine IP-Adresse wie 192.168.*.* oder 192.168.77.* verwenden.

Verwandte Themen anzeigen
Protokollierungswerkzeuge

# Kapitel 09: Erläuterung von Serverleistung und -wartung

## Serverleistung und Wartung

Eine Vielzahl von Faktoren beeinflussen die Leistung des Sametime Servers. Dieser Abschnitt enthält folgende Informationen und Tips:

- Nutzung von Serverressourcen
- Netzwerkauslastung und Serverbeschränkungen
- Einsatz einzelner und mehrerer Sametime Server
- Server-Tasks
- Die Datei Notes.ini
- Starten und Stoppen des Servers

Verwandte Themen anzeigen
Nutzung von Serverressourcen
Netzwerkauslastung und Serverbeschränkungen

## Nutzung von Serverressourcen

Für die Installation des Sametime Servers sind ungefähr 150 MB Speicherplatz plus Größe des Adreßbuchs erforderlich, das Datensätze für jedes Mitglied der Sametime Community enthält.

Der erforderliche Speicherplatz für den Server erhöht sich mit der Anzahl an Besprechungen, die in der Datenbank des Online-Besprechungszentrums (STCONF.NSF) angelegt werden, und der Anzahl und Größe der Diskussions- und anderer Sametime-aktivierter Datenbanken, die angelegt werden. Sie können den verfügbaren Plattenplatz mit Hilfe der Funktion "Überwachung - Speicherplatz" des Sametime Administrationswerkzeugs überwachen.

Lotus empfiehlt Ihnen, das Online-Besprechungszentrum (STCONF.NSF) häufig zu archivieren, damit seine Größe 1 GB nicht überschreitet.

Unter normalen Betriebsbedingungen benötigt der Sametime Server minimale CPU-Zyklen und RAM. Jedoch kann die Netzwerkbelastung erheblich variieren, je nach Art des gemeinsam benutzten Besprechungsinhalts und der Anzahl der Benutzer in einer Besprechung.

Der Community Server hat weniger Auswirkungen auf die Server-Ressourcenbelastung als der Besprechungsserver.

Verwandte Themen anzeigen
Netzwerkauslastung und Serverbeschränkungen

## Netzwerkauslastung und Serverbeschränkungen

Sametime generiert verschieden hohen Netzwerkverkehr, abhängig von den verwendeten Techniken der Zusammenarbeit. Beispielsweise beanspruchen die Sametime Funktionen für Chat und direkten Nachrichtenaustausch minimalen Netzwerkverkehr, aber der Einsatz der Pinwand in einer Online-Besprechung mit 100 Clients kann ein Netzwerk erheblich belasten. Zahlreiche Faktoren beeinflussen den Umfang des Netzwerkverkehrs, z. B. Server-Netzwerkverbindungen, Verarbeitungsgeschwindigkeit der Server-CPU, Größe der gemeinsamen Daten (Pinwand-Dateien, Inhalt gemeinsam genutzter Anwendungen), Client-Verbindungsgeschwindigkeiten und LAN-Topologie.

Aufgrund der Anzahl und Dynamik der beteiligten Variablen ist es schwierig, einen sinnvollen Wert für die maximale Anzahl unterstützter Clients an einem Sametime Server oder die maximal unterstützte Client-Anzahl in einer einzelnen Besprechung anzugeben.

Wenn Sie jedoch die folgenden Benutzungsrichtlinien beachten, sollten Sie in den meisten Situationen eine akzeptable Leistung des Sametime Servers erzielen:

- 8000 gleichzeitige Benutzer, die über Sametime Connect oder Chat-Funktionen von Sametime-aktivierten Datenbanken mit den Community Services verbunden sind
- 100 gleichzeitig aktive Online-Besprechungen
- 200 Benutzer pro aktiver Besprechung

Das Sametime Administrationswerkzeug umfaßt die Funktion "Protokolle - Protokollparameter". Mit dieser Funktion können Sie im Sametime Protokoll Warnmeldungen für den Fall generieren, daß die Serverbelastung angegebene Grenzen übersteigt.

Wenn die Serverleistung abfällt, können Sie in den Protokollen prüfen, ob das Problem durch zu viele Benutzer verursacht wird, die gleichzeitig auf den Server zugreifen. Sind keine Warnungen vorhanden, kann das Problem auch an der Anzahl von Clients liegen, die über langsame Verbindungen auf den Server zugreifen oder ungewöhnlich umfangreiche gemeinsame Dateien verwenden. Wenn die hohe Belastung die Serverleistung dauerhaft beeinträchtigt, sollten Sie einen weiteren Sametime Server hinzufügen. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server..

**Hinweis** Das Sametime Administrationswerkzeug umfaßt auch Überwachungsfunktionen, die sekundengenaue Statistiken über die Serverauslastung liefern.

Verwandte Themen anzeigen
Serverleistung und Wartung

## Einsatz einzelner und mehrerer Sametime Server

Dieser Abschnitt behandelt Themen über die Serverleistung beim Einsatz eines einzelnen und mehrerer Sametime Server.

### Einsatz eines einzelnen Servers

Wenn Sie einen einzelnen Sametime Server einsetzen, kann die Anzahl der Netzwerk-Router-Sprünge zwischen Clients und Server die Serverleistung beeinflussen. Sie sollten den Sametime Server in einen zentral positionierten Netzwerk-Backbone einbinden, um die Anzahl der erforderlichen Netzwerksprünge zwischen Clients und Server zu beschränken.

Beachten Sie beim Einsatz des Servers auch die Anzahl der langsameren WAN- (Wide Area Network) Sprünge und jeden potentiellen Client. Im Idealfall sollte gar kein oder nur ein WAN-Sprung pro möglicher Client-Server-Verbindung erforderlich sein. Sametime Clients, die für die Verbindung zum Server mehrere WAN-Sprünge benötigen, erzielen einen geringeren Durchsatz als Clients, die über ein LAN oder nur einen WAN-Sprung mit dem Server verbunden sind.

In einem umfangreichen Unternehmensnetzwerk ist es evtl. nicht möglich, die Anzahl der WAN-Sprünge für alle Clients zu reduzieren. In diesem Fall sollten Sie mehrere Sametime Server einsetzen und die Server als einzelne Community aktivieren. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server..

Der Sametime Server läuft unabhängig von seiner Umgebung reibungslos. Wenn Sie ihn jedoch physisch ideal plazieren, wird die Leistung optimiert.

### Einsatz mehrerer Server

Sie sollten mehrere Sametime Server einsetzen, wenn eine große Anzahl von Sametime Benutzern vorhanden ist oder die Netzwerktopologie mehrere WAN-Verbindungen enthält. Beim Einsatz mehrerer Server können Sie die Belastung durch eine hohe Benutzerzahl auf mehrere Sametime Server verteilen. Sie können auch die Sametime Server verbinden, um die Anzahl von WAN-Sprüngen zu reduzieren, die ein Client für die Teilnahme an einer Besprechung benötigt. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server..

Verwandte Themen anzeigen
Einsatz eines einzelnen Servers
Einsatz mehrerer Server

## Server-Tasks

Serverprogramme automatisieren komplexe Administrationsaufgaben, wie z. B. das Komprimieren von Datenbanken und das Aktualisieren von Indizes. Mit Hilfe der folgenden Methode können Sie ein Sametime Serverprogramm laufen lassen:

- Listen Sie das Programm in den Einstellungen "ServerTasks" oder "ServerTasksAt" der Datei NOTES.INI auf. Das Programm wird automatisch beim Startup des Servers geladen (oder zu einer bestimmten Stunde, die Sie festsetzen) und läuft, bis es die Aufgabe erfüllt oder bis der Server heruntergefahren wird.

Folgende Tabelle zeigt jedes Sametime Server Programm, den benötigten Serverbefehl, um es zu laden, eine kurze Beschreibung des Programms und die Standardeinstellung von NOTES.INI.

| Programm | Befehl | Beschreibung | NOTES.INI-Einstellung |
|---|---|---|---|
| Agent manager | AMgr | Führt Agents auf einer oder mehreren Datenbanken aus. | ServerTasks |
| Cataloger | Catalog | Aktualisiert den Datenbankkatalog. | ServerTasksAt1 |
| Chronos | Chronos | Aktualisiert Volltextindizes, für die stündliche, tägliche oder wöchentliche Aktualisierung eingestellt ist. | Keine |
| Collector | Collect | Sammelt Statistiken für mehrere Server. | Keine |
| Database compactor | Compact | Komprimiert alle Datenbanken auf dem Server, um ungenutzten Platz zu entfernen und Speicherplatz freizumachen. | Keine |
| Database fixup | Fixup | Findet und repariert beschädigte Datenbanken. | Keine |
| Designer | Design | Aktualisiert alle Datenbanken, um Änderungen für Schablonen anzuzeigen. | ServerTasksAt1 |
| Event | Event | Überwacht Ereignisse auf einem Server. | Keine |
| HTTP Server | HTTP | Aktiviert einen Sametime Server als Web-Server, so daß Browser-Clients auf Datenbanken auf dem Server zugreifen können. | Keine |
| Indexer | Updall | Aktualisiert alle geänderten Ansichten und/oder Volltextindizes für alle Datenbanken. | ServerTasksAt2 |
| Reporter | Report | Meldet Statistiken für einen Server. | Keine |
| Statistics | Statlog | Speichert die Datenbankaktivität in der Protokolldatei. | ServerTasksAt5 |
| Stats | Stats | Erstellt auf Anfrage Statistiken für einen entfernten Server. | ServerTasks |
| Web Retriever | Web | Implementiert das HTTP-Protokoll, um Web-Seiten abzurufen und in Notes Dokumente zu konvertieren. | Keine |

Verwandte Themen anzeigen
Serverleistung und Wartung

## Info über die NOTES.INI-Datei

Die Datei NOTES.INI ist ein Kontrollzentrum für einen Sametime Server. Sie stellt dem Sametime Server folgende Informationen zur Verfügung:

- Definiert alle Initialisierungseinstellungen für den Server.
- Erstellt eine Task-Liste, die der Server abarbeitet, wenn er startet.

Bei jedem Start überprüft der Server diese Datei auf Informationen über die auszuführenden Server-Tasks und die Einrichtung der Serverumgebung.

Die Konfigurationseinstellungen der Datei NOTES.INI sind anfangs anhand der Optionen eingestellt, die Sie während der Installation bzw. des Setups ausgewählt haben. Sie können die Einstellungen der Datei NOTES.INI wie folgt verändern:

- Bearbeiten Sie das Serverdokument mit dem Sametime Administrationswerkzeug.
- Erstellen oder bearbeiten Sie Server-Konfigurationsdokumente im Adreßbuch. Mit einem Server-Konfigurationsdokument können Sie eine Untergruppe für die NOTES.INI-Einstellungen für einen einzelnen Server, für eine Gruppe von Servern oder für alle Server in einer Community festsetzen.
- Bearbeiten Sie die Datei NOTES.INI in einem Texteditor. Die Datei NOTES.INI befindet sich im Windows- oder WinNT-Verzeichnis.

Wenn Sie die NOTES.INI-Einstellungen in einem Texteditor bearbeiten, können Dateifehler auftreten, die den Betrieb eines Sametime Servers behindern. Diese Methode, die Einstellungen NOTES.INI zu bearbeiten, wird nicht empfohlen.

Verwandte Themen anzeigen
Notes Protokoll

## Starten und Stoppen des Servers

Der Sametime Server läuft als Windows NT Service. Wenn Sie den Sametime Server starten oder stoppen möchten, folgen Sie nachstehenden Anleitungen.

So starten Sie den Sametime Server am Windows NT-Desktop:

- Wählen Sie "Start - Einstellungen - Systemsteuerung - Dienste".
- Klicken Sie im Dialogfeld "Dienste" auf "Sametime Server" und dann auf "Start".

So stoppen Sie den Sametime Server am Windows NT-Desktop:

- Wählen Sie "Start - Einstellungen - Systemsteuerung - Dienste".
- Klicken Sie im Dialogfeld "Dienste" auf "Sametime Server" und dann auf "Stop".

# Kapitel 10: Arbeiten mit mehreren Sametime Servern

## Verwenden mehrerer Sametime Server

Sie können mehrere Sametime Server in einer Domino Umgebung installieren. Der Installationsvorgang für einen zusätzlichen Sametime Server ist identisch mit dem für den ersten Sametime Server. Wenn jedoch diese Sametime Server miteinander kommunizieren sollen, müssen Sie sie zu einer einzelnen Community verbinden.

**Hinweis** Informationen über das Installieren eines Sametime Servers finden Sie im *Sametime Installationshandbuch*.

### Aktivieren mehrerer Sametime Server als einzelne Community

Wenn Sie mehrere Sametime Server so aktivieren, daß sie als einzelne Community fungieren, erscheinen sie Endbenutzern wie ein einziger Server. Der Einsatz mehrerer Server kann die Leistung von Sametime erhöhen, da sich die Belastung durch eine große Anzahl an Sametime Benutzern auf Systemressourcen auf zwei oder mehr Computern verteilen läßt.

Das Kombinieren mehrerer Sametime Server zu einer einzelnen Community gewährleistet, daß die Sametime Server dasselbe Adreßbuch verwenden und die Privacy-Einstellungen von Sametime Connect für alle Benutzer synchronisiert werden. Sie können auch den Mitgliedern der Community separate "lokale" Server zuweisen. Ein Benutzer baut eine Verbindung zu seinem lokalen Server auf, wenn er Sametime Connect Client verwendet oder mit Hilfe der Funktionen "Wer ist anwesend" oder "Wer ist online" einer Sametime-aktivierten Datenbank an Chat-Sitzungen teilnimmt. Durch das Zuweisen lokaler Server wird die Auslastung der Community Services auf die Server in der Sametime Community verteilt. Weitere Informationen finden Sie unter Aktivieren mehrerer Sametime Server als eine einzelne Community.

**Hinweis** Sie müssen Sametime in einer Domino Umgebung einsetzen, damit Sie mehrere Sametime Server als einzelne Community aktivieren können.

### Verbinden von Besprechungsservern

Wenn Sie mehrere Sametime Server als einzelne Community aktiviert haben, können Sie auch die Besprechungsserver mehrerer Sametime Server verbinden. Damit kann eine einzige Besprechung gleichzeitig auf zwei (oder mehr) Sametime Servern aktiv sein. Durch das Verbinden von Sametime Servern können Benutzer an unterschiedlichen geographischen Orten oder eine große Anzahl von Benutzern am selben Ort eine Verbindung zu verschiedenen Servern aufbauen, um an derselben Besprechung teilzunehmen. Verbundene Besprechungsserver verringern die Belastung der Netzwerkbandbreite und erhöhen die Server-Leistung. Sie können auch mehrere Server verbinden, um auf sichere Weise Besprechungen, die auf Sametime Servern innerhalb Ihres Firewalls geführt werden, auf Internet-Clients auszudehnen. Weitere Informationen finden Sie unter Verbinden mehrerer Besprechungsserver.

Verwandte Themen anzeigen

- Aktivieren mehrerer Sametime Server als eine einzige Community
- Verbinden von Besprechungsservern

## Aktivieren mehrerer Sametime Server als eine einzige Community

Wenn Sie mehrere Sametime Server installieren, können Sie mehrere Server als eine einzelne Community aktivieren. Dadurch können die Server miteinander kommunizieren und Sie können Online-Besprechungsserver verbinden.

**Hinweis** Der Installationsvorgang für einen zusätzlichen Sametime Server ist identisch mit dem für den ersten Sametime Server. Informationen über das Installieren eines Sametime Servers finden Sie im *Sametime Installationshandbuch*. Wenn Sie Sametime in einer reinen Web-Umgebung installiert haben (nur Web-Browser-Zugriff), lassen sich mehrere Sametime Server nicht als einzelne Community aktivieren. Ein Lotus Notes Client ist für diesen Prozeß erforderlich.

Um mehrere Sametime Server zu einer einzigen Sametime Community zusammenzufassen, sind folgende Prozeduren erforderlich:

1. Ändern Sie die Serverdokumente aller Sametime Server in der Domino Domäne.
2. Planen Sie Replizierung zwischen Sametime Servern in der Community.
3. Teilen Sie Benutzer auf die Sametime Server auf.

Verwandte Themen anzeigen
Verwenden mehrerer Sametime Server

## Ändern der Serverdokumente aller Sametime Server in der Domäne

Dies ist die erste von drei erforderlichen Prozeduren für das Aktivieren mehrerer Sametime Server als einzelne Community. Diese Prozedur stellt sicher, daß der Anschlußname jedes Sametime Servers korrekt auf TCPIP eingestellt ist. Sie können diese Prozedur auch im Sametime Administrationswerkzeug auf jedem Sametime Server oder auf einem Notes Client ausführen.

**Verwenden des Sametime Administrationswerkzeugs:**

1. Rufen Sie in Ihrem Web-Browser die Seite "Willkommen bei Sametime" auf dem Sametime Server auf.
2. Klicken Sie auf "Server Administration" und geben Sie Name und Kennwort des Administrators ein.
3. Wählen Sie "Server - Server".
4. Klicken Sie auf den Namen des Sametime Servers, um das Serverdokument zu öffnen. (Dieser Name sollte der Name des Sametime Servers ein, auf dem Sie das Sametime Administrationswerkzeug geöffnet haben.)
5. Klicken Sie auf "Server bearbeiten".
6. Blättern Sie im Serverdokument zum Abschnitt "Netzwerkkonfiguration ". Geben Sie im ersten Feld in der Spalte "Anschluß" den Eintrag "TCPIP" ein. (TCPIP sollte der Anschluß sein, den das TCPIP-Netzwerk verwendet.)
7. Blättern Sie an den Beginn des Serverdokuments und klicken Sie auf "Speichern und Schließen".
8. Wiederholen Sie diesen Vorgang für alle Sametime Server, die Sie zu einer einzelnen Community verbinden wollen.

**Verwenden eines Notes Client:**

1. Öffnen Sie auf einem Domino Server das Adreßbuch, das auf den Sametime Servern repliziert wird.
2. Wählen Sie "Server" und anschließend "Serveransicht".
3. Doppelklicken Sie auf den Namen des Sametime Servers.
4. Klicken Sie auf "Server bearbeiten", um das Serverdokument in den Bearbeitungsmodus zu bringen.
5. Öffnen Sie den Abschnitt "Netzwerkkonfiguration". Geben Sie in die erste Zeile dieses Abschnitts unter "Anschluß" den Eintrag "TCPIP" ein. (TCPIP sollte der Anschluß sein, den das TCPIP-Netzwerk verwendet.)
6. Klicken Sie auf "Speichern und Schließen", um diese Änderung im Sametime Serverdokument zu speichern.

7. Wiederholen Sie diesen Vorgang für alle Sametime Server, die Sie zu einer einzelnen Community verbinden wollen.

Erstellen Sie nach Ändern der Serverdokumente ein Verbindungsdokument, um die Replizierung der Privacy-Datenbank und des Adreßbuchs zu planen.

Verwandte Themen anzeigen
Aktivieren mehrerer Sametime Server als eine einzige Community

## Erstellen eines Verbindungdokuments für die periodische Replizierung zwischen Sametime Servern

Dies ist die zweite von drei erforderlichen Prozeduren für das Aktivieren mehrerer Sametime Server als einzelne Community. Sie müssen ein Verbindungsdokument anlegen, um periodische Replizierung zwischen Sametime Servern durchzuführen. Verwenden Sie eine Pull-Push-Replizierung zwischen den Sametime Servern.

Dieses Verbindungsdokument stellt sicher, daß Sametime Adreßbuch und Privacy-Datenbank (VPUSERINFO.NSF) zwischen Sametime Servern repliziert werden, um eine einheitliche Sametime Community zu erhalten.

**Hinweis** Das Sametime Administrationswerkzeug bietet eine Funktion, über die Sie ein Verbindungsdokument für die Verbindung zweier Sametime Besprechungsserver erstellen können. Beim nachstehend beschriebenen handelt es sich um ein anderes Verbindungsdokument, da es periodische Replizierung festlegt. Das Verbindungsdokument, das Verbindungsdokument, das mit Hilfe des Sametime Administrationswerkzeugs angelegt wurde, ermöglicht, daß eine einzige Besprechung auf zwei Sametime Servern aktiv ist. Weitere Informationen finden Sie unter Verbinden von Besprechungsservern.

Führen Sie im Lotus Notes Arbeitsbereich auf einem Domino Server folgende Schritte aus:

1. Öffnen Sie das Öffentliche Adreßbuch auf dem Domino Server.
2. Wählen Sie die Verbindungsansicht und klicken Sie auf "Add Connection".

   Füllen Sie die erforderlichen Felder im Verbindungsdokument aus. In nachstehendem Beispiel entspricht der eine Sametime Server "STBoston01" und der andere "STBoston02". Die Server befinden sich in der ACME-Domäne.

   Beispiel für ein Verbindungsdokument:

   | | |
   |---|---|
   | Connection Type: | LAN |
   | Source Server: | STBoston01/ACME |
   | Destination Server: | STBoston02/ACME |
   | Source Domain | ACME |
   | Destination Domain: | ACME |
   | Scheduled: | Enabled |
   | Tasks: | Replication |
   | Call Times: | 12:01 AM - 11:59 PM |
   | Repeat Interval | 60 Minutes |
   | Days: | Sun, Mon, Tues, Wed, Thu, Fri, Sat |
   | Replication Type: | Pull Push |

3. Klicken Sie auf "Save and Close".
4. Wiederholen Sie obigen Vorgang, um Verbindungsdokumente zwischen einem Sametime Server (in obigem Beispiel STBoston01) und jedem weiteren Sametime Server anzulegen, der der Community angehören soll.
5. Schließen Sie das Öffentliche Adreßbuch.

Nach Erstellen der Verbindungsdokumente können Sie Benutzer auf die Sametime Server verteilen.

Verwandte Themen anzeigen
Aktivieren mehrerer Sametime Server als eine einzige Community
Verteilen von Benutzern auf mehrere Sametime Server

## Verteilen von Benutzern auf mehrere Sametime Server

Um Benutzer auf mehrere Sametime Server zu verteilen, muß der Administrator den lokalen Sametime Server für jeden Benutzer in der Sametime Community angeben. Der lokale Server ist derjenige, auf den jeder Benutzer zugreift, wenn er Online-Awareness und Chat-Funktionen in Sametime Connect und in Sametime Diskussionen, Dokumentbibliotheken oder E-Mail-Anwendungen verwendet.

Geben Sie im Adreßbuch auf einem Sametime Server den Namen des Servers in das Feld "Sametime Server" am Ende des Personendokuments eines jeden Benutzers ein. Sie sollten zu diesem Zweck einen einfachen Agent erstellen.

**Hinweis** Wenn Sie im Sametime Administrationswerkzeug einen Benutzer über den Befehl "Benutzer - Benutzer hinzufügen" aufnehmen, wird das Feld "Sametime Server" automatisch mit dem Namen des Servers ausgefüllt, auf dem das Sametime Administrationswerkzeug läuft.

Der Sametime Connect Client umfaßt auf dem lokalen Computer jedes Benutzers auch Verbindungseinstellungen. Der Benutzer kann auf diese Einstellungen zugreifen, indem er bei der Anmeldung bei Sametime Connect die Option "Anschlußmöglichkeit" wählt oder indem er in Sametime Connect "Optionen - Vorgaben - Sametime Anschlußmöglichkeit" wählt.

Das Feld "Host:" in den Sametime Verbindungseinstellungen des Sametime Connect Client muß denselben Server angeben wie das Feld "Sametime Server" im Personendokument des Benutzers. Verwenden Sie im Personendokument das Lotus Notes Format "servername/domänenname" (z. B. server1/acme) um den Server anzugeben. Verwenden Sie im Feld "Host:" der Sametime Verbindungseinstellungen den DNS-Namen oder die IP-Adresse des Sametime Servers (z. B. server.acme.com oder 100.100.10.10.

Sie haben die Prozeduren abgeschlossen, die zur Aktivierung mehrerer Sametime Server als einzelne Community erforderlich sind. Optional können Sie für alle Sametime Server, die in der Umgebung installiert sind, die Sicherheit erhöhen.

Verwandte Themen anzeigen
Verteilen von Belastung und Nutzung des Netzwerks

## Verbinden von Besprechungsservern

Wenn Sie mehrere Sametime Server als einzelne Community aktiviert haben, kann der Administrator Verbindungsdokumente erstellen, um die Besprechungsserver unterschiedlicher Sametime Server miteinander zu verbinden.

Das Verbinden der Besprechungsserver bietet folgende Vorteile:

- Erhöhen der Besprechungsserver-Leistung, wenn eine große Zahl von Sametime Benutzern vorhanden ist
- Optimieren der Netzwerkauslastung

Durch das Verbinden von Besprechungsservern kann eine einzige Besprechung gleichzeitig auf zwei (oder mehr) Sametime Servern aktiv sein. Dabei können Benutzer an unterschiedlichen geographischen Orten oder eine große Anzahl von Benutzern am selben Ort eine Verbindung zu verschiedenen Servern aufbauen, um an derselben Besprechung teilzunehmen.

Das Verbinden von Besprechungsservern ermöglicht auch, daß Besprechungen auf einem Sametime Server innerhalb Ihres Firewalls auf einen Sametime Server außerhalb des Firewalls ausgedehnt werden. Dadurch können Internet-Clients an internen Besprechungen teilnehmen, ohne den Firewall zu überqueren. Weitere Informationen finden Sie unter Firewalls und Sametime Internet -Server.

Für das Verbinden von Servern muß der Administrator mit Hilfe des Sametime Administrationswerkzeugs ein Verbindungsdokument erstellen, der eine Verbindung zwischen den beiden Servern aufbaut.

Sobald der Administrator zwei Besprechungsserver verbunden hat, werden dem Formular "Neue Besprechung" im Online-Besprechungszentrum die folgenden beiden Optionen hinzugefügt:

- Teilnehmer können von Sametime Servern innerhalb des Unternehmens teilnehmen "Teilnehmer können von Sametime Servern innerhalb des Unternehmens teilnehmen"
- Teilnehmer aus dem Internet können teilnehmen

Wenn der Endbenutzer beim Anlegen einer neuen Besprechung eine dieser Optionen wählt, wird die Besprechung auf den verbundenen Servern aktiv.

Die Option "Teilnehmer können von Sametime Servern innerhalb des Unternehmens teilnehmen" verbindet Server, die der Administrator manuell innerhalb des Firewalls festgelegt hat. Die Option "Teilnehmer aus dem Internet können teilnehmen" verbindet Server, die der Administrator manuell außerhalb des Firewalls festgelegt hat.

Verwandte Themen anzeigen
Vorteile beim Verbinden mehrerer Online-Besprechungsserver
Verteilen von Belastung und Nutzung des Netzwerks
Firewalls und Sametime Internet-Server
Aktivieren mehrerer Sametime Server als eine einzige Community

### Vorteile beim Verbinden mehrerer Online-Besprechungsserver

Die Verbindung von Online-Besprechungsservern bietet folgende Vorteile:

- Sie können die von einer großen Zahl an Sametime Benutzern verursachte Belastung der Systemressourcen auf zwei (oder mehr) Computer verteilen.
- Die Belastung der Netzwerkbandbreite wird reduziert.
- Internet-Clients können an Besprechungen auf einem Sametime Server hinter Ihrem Firewall teilnehmen, ohne die Sicherheit Ihres Netzwerks zu gefährden.

Verwandte Themen anzeigen
Verteilen von Belastung und Nutzung des Netzwerks
Firewalls und Sametime Internet-Server

### Verteilen von Belastung und Nutzung des Netzwerks

Wenn Sie mehrere Sametime Server in einer Domino Umgebung installiert und die Server als einzelne Community aktiviert haben, können Sie die Besprechungsserver verbinden, um die Leistung zu verbessern. Durch Verbinden von Besprechungsservern können die Systemressourcen mehrerer Server eine große Zahl an Sametime Benutzern unterstützen. Auch die Nutzung der Netzwerkbandbreite wird durch Verbinden von Besprechungsservern reduziert.

Nehmen Sie zum Beispiel an, Sie verfügen über eine WAN-Umgebung, die Boston und Dublin versorgt. Sie können einen Sametime Server an jedem Ort installieren und die Server verbinden. Ein Endbenutzer kann dann auf dem Sametime Server in Dublin eine Online-Besprechung anlegen. Am geplanten Anfangszeitpunkt wird die Besprechung auf dem Server in Dublin und auf dem Server in Boston aktiv. Benutzer in Dublin können auf dem Server in Dublin und Benutzer in Boston auf dem Server in Boston an der Besprechung teilnehmen.

**Hinweis** Beim Anlegen einer Besprechung bestimmt der Endbenutzer, ob die Besprechung auf einem verbundenen Server aktiv wird, indem er die entsprechende Option im Formular "Neue Besprechung" aktiviert.

Diese Möglichkeit bietet zwei Vorteile:

- Die Systemressourcen von zwei Computern teilen sich die Belastung durch die Online-Besprechung. Daher können Meeting Services auf jedem Sametime Server effizienter arbeiten und die Besprechungsleistung für den Endbenutzer wird erhöht.
- Die Belastung der Netzwerkbandbreite wird verringert, da einzelne Clients die WAN-Verbindung nicht benötigen, um an der Besprechung teilzunehmen. Die Benutzer in Boston bauen eine Verbindung zum LAN in Boston auf und die Benutzer in Dublin zum LAN in Dublin.

  Wenn zwei Server verbunden werden, wird eine einzige T.120-Verbindung zwischen den beiden Servern am T.120-Kommunikationsanschluß des Servers (standardmäßig Anschluß 1503) aufgebaut. Sämtliche Daten der Online-Besprechung werden über diese eine Verbindung übertragen.

Anschluß 1503 ist in den Besprechungsserver-Netzwerkeinstellungen des Sametime Administrationswerkzeugs als T.120-Server-Kommunikationsanschluß eingestellt.

Verwandte Themen anzeigen
Vorteile beim Verbinden mehrerer Online-Besprechungsserver
Firewalls und Sametime Internet-Server

## Firewalls und Sametime Internet-Server

Die Plazierung des Sametime Servers in Relation zum Firewall beeinflußt, wie Sametime Online-Besprechungsserver verbunden werden. Wenn zwei Sametime Server verbunden werden, passieren alle Daten zwischen den Servern über den Anschluß, der auf der Administrationsseite "Netzwerk und Sicherheit" des Sametime Administrationswerkzeugs als T.120-Server-Kommunikationsanschluß (standardmäßig 1503) eingestellt ist.

Sametime Server verlangt, daß noch mehrere andere Anschlüsse für Client-Zugriff auf den Server geöffnet sind. Wenn Ihr Sametime Server hinter einem Firewall eingesetzt wird, kann das Öffnen mehrerer Anschlüsse durch den Firewall für Client-Zugriff zu Sicherheitsrisiken führen.

Sie können zwei (oder mehr) Sametime Server einsetzen und die Online-Besprechungsserver verbinden, um Internet-Clients die Teilnahme an Besprechungen zu ermöglichen, die auf einem Sametime Server innerhalb des Firewalls geführt werden. Setzen Sie z. B. Sametime Server A innerhalb des Unternehmens-Firewalls ein und Sametime Server B außerhalb des Firewalls. Öffnen Sie Anschluß 1503 zwischen den beiden Servern und legen Sie ein Verbindungsdokument an, um die beiden Online-Besprechungsserver zu verbinden. Wenn eine Besprechung auf Sametime Server A gestartet wird, wird diese Besprechung auch auf Sametime Server B aktiv. Internet-Clients können auf Server B zugreifen und an der Besprechung teilnehmen, ohne den Firewall zu überqueren.

**Hinweis** Wenn zwei Server verbunden sind, bestimmt der Endbenutzer beim Anlegen einer Besprechung, ob diese Besprechung auf dem verbundenen Server aktiv wird. Weitere Informationen finden Sie unter Anlegen einer Besprechung auf verbundenen Servern.

Wenn Sie einen Sametime Server außerhalb des Firewalls einsetzen, können Sie über die ACL der Datenbank für das Sametime Besprechungszentrum (STCONF.NSF) die Privilegien steuern, über die Internet-Clients am Server verfügen. Stellen Sie z. B. anonymen und Standardzugriff auf "Leser" ein, um Internet-Clients die Teilnahme an Besprechungen jedoch nicht das Anlegen von Besprechungen zu gestatten. Wenn anonymer und Standardzugriff im Besprechungszentrum auf "Autor" eingestellt sind, können Internet-Clients neue Online-Besprechungen auf dem Server außerhalb des Firewalls anlegen.

Verwandte Themen anzeigen
Vorteile beim Verbinden mehrerer Online-Besprechungsserver
Verteilen von Belastung und Nutzung des Netzwerks

## Anlegen einer Besprechung auf verbundenen Servern

Der Endbenutzer oder der Besprechungsverwalter verwendet das Formular "Neue Besprechung", um eine neue Besprechung im Sametime Besprechungszentrum anzulegen. Wenn der Administrator Besprechungsserver verbunden hat, werden dem Formular "Neue Besprechung" im Sametime Besprechungszentrum die folgenden beiden Optionen hinzugefügt:

- Benutzern erlauben, von Servern innerhalb des Unternehmens teilzunehmen
- Benutzern erlauben, vom Internet teilzunehmen

**Hinweis** Wenn der Administrator die Server nicht verbunden hat, erscheinen die beiden Optionen nicht im Formular "Neue Besprechung".

Wenn der Besprechungsverwalter die Option "Benutzern erlauben, von Servern innerhalb des Unternehmens teilzunehmen" wählt, wird die Besprechung innerhalb des Unternehmens-Firewalls auf allen Servern aktiv, mit denen der Sametime Server verbunden ist. Wenn der Besprechungsverwalter die Option "Benutzern erlauben, vom Internet teilzunehmen" wählt, wird die Besprechung außerhalb des Unternehmens-Firewalls auf allen Servern aktiv, mit denen der Sametime Server verbunden ist. Weitere Informationen finden Sie unter Firewalls und Sametime Internet-Server.

Verwandte Themen anzeigen
Erstellen von Verbindungsdokumenten für das Verbinden von Besprechungsservern

## Erstellen von Verbindungsdokumenten für das Verbinden von Besprechungsservern

Wenn Sie mehrere Sametime Server installiert und als einzelne Community aktiviert haben, können Sie die Server verbinden, indem Sie Verbindungsdokumente anlegen.

So legen Sie ein Verbindungsdokument an, um zwei Besprechungsserver zu verbinden:

1. Wählen Sie "Server-Administration" auf der Seite "Willkommen bei Sametime" und geben Sie Name und Kennwort des Administrators ein.
2. Wählen Sie "Server" und dann "Meeting Services".
3. Wählen Sie "Verbindungsdokumente erstellen". Die Seite "Neue Verbindung hinzufügen" wird angezeigt.
4. Füllen Sie die Felder auf dieser Seite aus und klicken Sie auf "Speichern".

   Die Seite "Neue Verbindung hinzufügen" enthält die folgenden Felder:

   **Quellserver** - Geben Sie den Namen des lokalen Servers im Domino Server Namensformat an, das den Domänen- oder Community-Namen enthält (z. B. sametimeA.acme.com/ACME, wobei ACME der Domänenname ist). Der lokale Server ist der Server, auf dem der Besprechungsverwalter die Besprechung anlegt.

   **Zielserver** - Geben Sie den Namen des Zielservers im Domino Server Namensformat an, das den Domänen- oder Community-Namen enthält. Der Zielserver ist der entfernte Server, auf dem die Besprechung aktiv wird. (Die Besprechung wird auf dem lokalen Server erstellt und wird auf dem lokalen und dem Zielserver aktiv.)

   Beim Anlegen eines Verbindungsdokuments, der Server A als lokalen Server und Server B als Zielserver angibt, wird die auf Server A angelegte Besprechung auf Server B nur dann aktiv, wenn der Besprechungsverwalter die entsprechende Option im Formular "Neue Besprechung" aktiviert. Der Besprechungsverwalter trifft diese Wahl, wenn er eine neue Besprechung anlegt.

   Jedoch kann eine Besprechung, die auf Server B angelegt wird, nicht auf Server A aktiv werden. Wenn Besprechungen, die auf Server B gestartet werden, auf Server A aktiv werden sollen, müssen Sie einen separaten neues Verbindungsdokument erstellen, der Server B als lokalen Server und Server A als Zielserver angibt.

   **Verbindungen zulassen** - Sie können eine oder beide Optionen unter "Verbindungen zulassen" aktivieren.

   - Wenn das Verbindungsdokument zwei Server verbindet, die sich innerhalb des Firewalls befinden, aktivieren Sie "Innerhalb meines Unternehmens".
   - Wenn das Verbindungsdokument einen Server innerhalb des Firewalls mit einem Server außerhalb des Firewalls verbindet, aktivieren Sie "Vom Internet".

   Wenn Sie "Vom Internet" aktivieren, sollten Sie einen Server außerhalb des Firewalls manuell festgelegt und Anschluß 1503 zwischen den beiden Servern geöffnet haben.

   **Optionale Netzwerkadresse** - Optional können Sie den vollständigen DNS-Namen oder die IP-Adresse des Zielservers in dieses Feld eingeben.

Verwandte Themen anzeigen
Details: Erstellen von Verbindungsdokumenten

## Details: Erstellen von Verbindungsdokumenten

Die Einstellungen unter "Verbindungen zulassen" im Formular "Neue Verbindung hinzufügen" haben keine Auswirkung auf Ihre aktuelle Firewall-Konfiguration. Sie dienen lediglich der Vereinfachung der Benutzeroberfläche für den Endbenutzer.

Die Einstellungen unter "Verbindungen zulassen" haben ebensowenig Auswirkungen auf die Verbindungsmechanik zwischen den beiden Servern. Wenn Sie ein Verbindungsdokument für die Verbindung zweier Server erstellen, werden die Server über Anschluß 1503 verbunden, unabhängig davon, ob für die Verbindung "Innerhalb meines Unternehmens" oder "Vom Internet" gewählt ist.

Sie müssen die Sametime Server manuell innerhalb des Firewalls ("Innerhalb meines Unternehmens") oder außerhalb des Firewalls ("Vom Internet") festlegen und Anschluß 1503 manuell zwischen den beiden Servern

öffnen.

Wenn Sie ein Verbindungsdokument für zwei Server erstellen, sollte die Einstellung unter "Verbindungen zulassen" den physischen Einsatz der Server reflektieren. Wenn Sie z. B. die beiden Server innerhalb des Firewalls einsetzen, sollten Sie "Innerhalb meines Unternehmens" aktivieren. Wenn einer der beiden Server außerhalb des Firewalls eingesetzt wird, aktivieren Sie "Vom Internet".

Wenn der Besprechungsverwalter eine Besprechung anlegt und die Einstellung "Innerhalb meines Unternehmens" auf dem Formular "Neue Besprechung" wählt, liest der Besprechungsserver alle Verbindungsdokumente im Adreßbuch und baut eine Verbindung zu den Servern auf, für die "Innerhalb meines Unternehmens" im Verbindungsdokument angegeben ist. Der Besprechungsserver kann nicht unterscheiden, ob sich der Server physisch innerhalb oder außerhalb des Firewalls befindet.

Beim Erstellen der Besprechung braucht der Besprechungsverwalter nur zu entscheiden, ob Clients aus dem Internet oder innerhalb des Unternehmensnetzwerks teilnehmen dürfen. Dadurch werden dem Endbenutzer die komplexen Vorgänge bei der Verbindung von Servern erspart.

Sie können auch an einem Lotus Notes Client ein Verbindungsdokument erstellen, der zwei Sametime Besprechungsserver verbindet. Öffnen Sie hierfür das Öffentliche Adreßbuch auf einem Sametime Server. Verwenden Sie die übliche Domino Prozedur, um ein neues Verbindungsdokument anzulegen. Geben Sie im Verbindungsdokument den lokalen und den Zielserver an, wählen Sie den Verbindungstyp "Sametime" und aktivieren Sie die Einstellung "Within the organization" oder "From the Internet" unter "Allow Connections". Der Sametime Verbindungstyp baut eine Verbindung zwischen den beiden Servern über Anschluß 1503 auf.

## Bearbeiten und Löschen von Verbindungsdokumenten

Sie können bestehende Verbindungsdokumente bearbeiten oder löschen. Beim Bearbeiten eines Verbindungsdokuments können Sie die Optionen unter "Verbindungen zulassen" und die "Optionale Netzwerkadresse" für den Zielserver ändern. Die Felder für den lokalen oder den Zielserver können Sie nicht ändern.

Durch Löschen des Verbindungsdokuments wird die Verbindung zwischen zwei Servern getrennt.

### So bearbeiten Sie ein Verbindungsdokument:

1. Wählen Sie "Server-Administration" auf der Seite "Willkommen bei Sametime" und geben Sie Name und Kennwort des Administrators ein.
2. Wählen Sie "Server" und dann "Meeting Services".
3. Wählen Sie "Verbindungsdokumente verwalten".
4. Bearbeiten Sie das gewünschte Feld und klicken Sie auf "Speichern".

### So löschen Sie ein Verbindungsdokument:

1. Wählen Sie "Server-Administration" auf der Seite "Willkommen bei Sametime" und geben Sie Name und Kennwort des Administrators ein.
2. Wählen Sie "Server" und dann "Meeting Services".
3. Wählen Sie "Verbindungsdokumente verwalten".
4. Wählen Sie den Verbindungsdokumente aus und klicken Sie auf "Löschen".

Verwandte Themen anzeigen

Erstellen von Verbindungsdokumenten für das Verbinden von Besprechungsservern

## Erhöhen der Sicherheit für einzelne oder mehrere Sametime Server

Wenn Sie einen Sametime Server in einer Domino Umgebung oder mehrere Sametime Server installiert haben, können Sie die Sicherheit für die Sametime Server erhöhen. Dabei handelt es sich um eine **optionale** Prozedur, die zusätzlichen Schutz vor unbefugten Benutzern bietet, die auf den Sametime Server zugreifen wollen. Durch diese Prozedur wird der Authentifizierungsprozeß für Benutzer komplexer, die eine Verbindung zu Community Services und Meeting Services aufbauen.

Sametime Server verwenden bei der Authentifizierung von Benutzern eine Secrets-Datenbank (STAuthS.nsf). Für größtmögliche Sicherheit können Sie die Secrets-Datenbank auf einem Sametime Server aktivieren, um Secrets zu generieren, und diese Secrets-Datenbank auf allen anderen Sametime Servern in der Community replizieren.

**Hinweis** Wenn Sie die folgenden Schritte auf einem anderen als einem Sametime Server ausführen, müssen Sie über den Agent-Zugriff "Beschränkt ausführen" und "Unbeschränkt ausführen" auf den Sametime Server verfügen. Andernfalls ist die Signierung des Agent und der Datenbank nicht korrekt und die Authentifizierung wird nicht problemlos ablaufen.

So erhöhen Sie die Sicherheit:

1. Aktivieren Sie die Generierung von Secrets auf einem Sametime Server.

   Schritt 1 ist der einzige erforderliche Schritt, um die Sicherheit für einen einzelnen Sametime Server zu erhöhen.

2. Replizieren Sie Secrets, um die Sicherheit für mehrere Sametime Server zu erhöhen.

Wenn Sie den Agent "SametimeSecretsGenerator" in einer Secrets-Datenbank auf einem Sametime Server aktiviert haben, müssen Sie diese Secrets-Datenbank auf allen anderen Sametime Servern in der Community replizieren.

## Aktivieren des Agent zur Secrets-Generierung

Dies ist die erste von zwei erforderlichen Prozeduren zur Erhöhung der Sicherheit von mehreren Sametime Servern, die in einer einzigen Community laufen. Um die Sicherheit von mehreren Sametime Servern zu erhöhen, müssen Sie den Agent "SametimeSecretsGenerator" auf einem Sametime Server aktivieren.

Wenn Sie die Sicherheit für eine Sametime-aktivierte Anwendung auf einem Domino Server erhöht haben, wurde diese Prozedur bereits ausgeführt, d. h. Sie müssen Sie nicht mehr ausführen. Allerdings müssen Sie die Secrets-Datenbank, in der der Agent zur Generierung von Secrets aktiviert ist, auf den anderen Sametime Servern aktivieren. Ermitteln Sie den Sametime Server, auf dem der Agent zur Secrets-Generierung aktiviert ist, und führen Sie die Prozedur unter Replizieren von Secrets zur Erhöhung der Sicherheit für mehrere Sametime Server aus.

**Hinweis** Wenn Sie den Agent zur Secrets-Generierung auf einem anderen als einem Sametime Server aktivieren, müssen Sie über den Agent-Zugriff "Beschränkt ausführen" und "Unbeschränkt ausführen" auf den Sametime Server verfügen. Andernfalls ist die Signierung des Agent und der Datenbank nicht korrekt und die Authentifizierung wird nicht problemlos ablaufen.

So aktivieren Sie den Agent SametimeSecretsGenerator:

1. Öffnen Sie auf dem Sametime Server, der Secrets generieren wird, die Secrets-Datenbank (STAuthS.nsf).
2. Wählen Sie aus dem Menü "Ansicht" die Option "Agenten".
3. Klicken Sie in das Markierungsfeld links neben dem Agent "SametimeSecretsGenerator". Stellen Sie sicher, daß "Lokal" ausgewählt ist. Klicken Sie auf OK.

Wenn nur ein Sametime Server in der Domäne installiert ist, ist dies die einzige erforderliche Prozedur zur Erhöhung der Sicherheit für Community Server und Besprechungsserver-Clients.

Wenn mehrere Sametime Server installiert sind, siehe Replizieren von Secrets zur Erhöhung der Sicherheit für mehrere Sametime Server, um den Vorgang abzuschließen.

## Replizieren von Secrets zur Erhöhung der Sicherheit für mehrere Sametime Server

Dies ist die letzte von zwei erforderlichen Prozeduren zur Erhöhung der Sicherheit für mehrere Sametime Server, die in einer einzigen Community laufen.

Sie müssen eine einmalige Replik der Sametime Secrets-Datenbank auf allen Sametime Servern anlegen, die als einzelne Community aktiviert sind. Ein Sametime Server muß als lokaler Server für die Secrets-Datenbank dienen. Am einfachsten verwenden Sie den Sametime Server, von dem aus Sie das Adreßbuch für andere Sametime Server repliziert haben. Die Verbindungsdokumente, die Sie angelegt haben, um das Adreßbuch zu replizieren, werden automatisch die Secrets-Datenbank replizieren.

So legen Sie eine einmalige Replik der Sametime Secrets-Datenbank auf einem Sametime Server an:

1. Öffnen Sie Lotus Notes auf dem Sametime Server, auf dem Sie eine Replik der Secrets-Datenbank anlegen wollen. Wählen Sie auf dem Windows-Desktop "Start - Ausführen" und geben Sie "Notes" ein.
2. Stellen Sie sicher, daß keine Datenbanksymbole ausgewählt sind.
3. Wählen Sie "Datei - Replizierung - Neue Replik".
4. Wählen Sie den Sametime Server, auf dem Sie den Agent "SametimeSecretsGenerator" aktiviert haben.
5. Geben Sie in das Feld für den Dateinamen "STAuthS.nsf" ein, um die Secrets-Datenbank zu replizieren.
6. Klicken Sie auf "Öffnen". Das Dialogfeld "Neue Replik" wird angezeigt.
7. Wählen Sie im Abschnitt "Erstellen" die Option "Sofort" und stellen Sie sicher, daß die Option "Zugriffskontrolliste kopieren" aktiviert ist.
8. Klicken Sie auf OK. Wenn Sie aufgefordert werden, die bestehende Secrets-Datenbank zu ersetzen, klicken Sie auf "Ja".
9. Wiederholen Sie diese Schritte, um eine einmalige Replik der Secrets- (STAuthS.nsf) Datenbank auf jedem Sametime Server anzulegen, auf dem Sie die Sicherheit erhöhen wollen. Das Verbindungsdokument, in dem Sie die Sametime Server als einzelne Community aktiviert haben, plant die Replizierung der Secrets-Datenbank wie erforderlich.

Damit ist der Prozeß abgeschlossen, bei dem die Sicherheit für mehrere Sametime Server, die als einzelne Community aktiviert sind, erhöht wird.

# Kapitel 11: Eräuterung von Sametime Sicherheit

## Info über Sametime Sicherheit

Der Sametime Server besitzt dieselben Sicherheitsfunktionen für Internet und Intranet, die auch in einem Domino Server zur Verfügung stehen. Wenn Sie den Sametime Server ausschließlich als Web-Server einsetzen und mit dem Domino Internet- und den Intranet-Sicherheitssystemen nicht vertraut sind, sollten Sie den Abschnitt über Sicherheit vollständig lesen, bevor Sie die Standard-Sicherheitseinstellungen auf dem Sametime Server ändern.

Neben den Sicherheitsfunktionen für Domino Internet und Intranet beinhaltet der Sametime Server Sicherheitsvorkehrungen für die Authentifizierung von Verbindungen zwischen Sametime Benutzern und Services für Besprechungen sowie Community Services. Eine kurze Beschreibung hierzu erhalten Sie unter Authentifizierung von Verbindungen zum Sametime Server.

**Hinweis** Der Abschnitt "Sicherheit" im Sametime Administratorhandbuch erklärt Internet- und Intranet-Sicherheitsfunktionen. Sicherheitsinformationen für Notes Benutzer finden Sie in der Administrationsdokumentation von Domino.

Verwandte Themen anzeigen
- Internet- und Intranet-Sicherheit
- Maximierung von Internet- und Intranet-Sicherheit für den Sametime Server

## Einführung in Sametime Sicherheit

Der Sametime Server umfaßt ausführliche und extrem anpaßbare Sicherheitsfunktionen. Dieser Abschnitt bietet Sicherheitsinformation, um Ihnen den Einstieg in Sametime zu erleichtern.

### Anonymer Zugriff auf das Sametime Besprechungszentrum

Standardmäßig ist anonymer Zugriff auf das Sametime Besprechungszentrum erlaubt. Ein beliebiger Benutzer kann eine Besprechung anlegen, ohne einen Benutzernamen oder ein Kennwort einzugeben. Zur strengeren Kontrolle können Sie den anonymen Zugriff auf das Besprechungszentrum ausschalten. Weitere Informationen finden Sie unter Deaktivieren des anonymen Zugriffs auf das Sametime Besprechungszentrum.

### Die Funktion "Selbstregistrierung"

Der Sametime Server gestattet Benutzern, sich selbst als Mitglied der Sametime Community zu registrieren. Mit Hilfe dieser Funktion kann ein beliebiger Benutzer Personendokumente im Adreßbuch anlegen und Sametime Connect verwenden. Bedenken Sie die Folgen für die Sicherheit, bevor Sie die Verwendung dieser Funktion gestatten. Weitere Informationen finden Sie unter Verwenden der Selbstregistrierung.

### Unterdrücken von Sicherheitsalarmen

Beim Einsatz von Sametime in einer Domino Umgebung können Benutzer von Notes R5 bei ihrer ersten Teilnahme an einer Online-Besprechung "Sicherheitsalarm" erhalten. Wie Sie diese Warnungen unterdrücken und wie Benutzer darauf reagieren sollten, erfahren Sie unter Ändern der Administrator ECL für Lotus Notes R5 Clients.

Verwandte Themen anzeigen
- Deaktivieren des anonymen Zugriffs auf das Online-Besprechungszentrum
- Verwenden der Selbstregistrierung
- Ändern der Administrator-ECL für Lotus Notes R5 Clients

### Deaktivieren des anonymen Zugriffs auf das Online-Besprechungszentrum

Die Standardeinstellungen der Sametime Sicherheit gestatten Benutzern von Web-Browsern, anonym auf die Datenbank des Sametime Besprechungszentrums (STCONF.NSF) zuzugreifen. Dies bedeutet, daß die Benutzer weder einen Benutzernamen noch ein Kennwort eingeben müssen.

Zur Erhöhung der Sicherheit für das Besprechungszentrum können Sie den anonymen Zugriff deaktivieren. Alle Benutzer müssen dann einen Benutzernamen und ein Kennwort eingeben, wenn sie auf das Sametime Besprechungszentrum zugreifen. Benutzer von Web-Browsern geben den Benutzernamen und das Internet-Kennwort ihres Personendokuments ein. Lotus Notes Clients verwenden denselben grundlegenden Kennwort-Authentifizierungsprozeß wie Domino Server.

Den anonymen Zugriff auf das Sametime Besprechungszentrum (STCONF.NSF) deaktivieren Sie wie folgt:

1. Wählen Sie "Server-Administration" auf der Seite "Willkommen bei Sametime".
2. Geben Sie Administratorname und -kennwort ein.
3. Wählen Sie "Server" und dann "Datenbanksicherheit".
4. Wählen Sie "Sametime Online-Besprechungszentrum" aus der Datenbankliste.
5. Klicken Sie auf die Schaltfläche "Zugriff".
6. Wählen Sie den Eintrag "Anonym" aus.
7. Wählen Sie im Zugriffsfeld die Ebene "Kein Zugriff" für den Eintrag "Anonym".
8. Klicken Sie auf "Senden".

Nach Ausführen dieser Schritte erhalten Benutzer die Standard-Zugriffsebene in der Zugriffskontrolliste (ACL) des Besprechungszentrums. Die Standard-Zugriffsebene ist "Autor", die jedem Benutzer, der ein Kennwort eingibt, Privilegien des Besprechungsverwalters verleiht (die Möglichkeit, Besprechungen anzulegen und zu ändern).

Sie können die Sicherheit noch strenger kontrollieren, indem Sie festlegen, welche Benutzer über Privilegien des Besprechungsverwalters oder nur über Teilnehmerprivilegien verfügen. Hierfür müssen Sie einzelne Benutzernamen oder Gruppennamen in die ACL des Online-Besprechungszentrums eingeben und jedem Namen entweder das Privileg "Autor" (Besprechungsverwalter) oder das Privileg "Leser" (nur Teilnehmer) zuweisen. Sie müssen auch sicherstellen, daß "Anonym" und "Standard" in der Datenbank-ACL auf "Kein Zugriff" eingestellt sind.

Verwandte Themen anzeigen
Einrichten der grundlegenden Kennwortauthentifizierung in einer Datenbank-Zugriffskontrolliste (ACL)
Hinzufügen von Benutzern zu einer Datenbank-Zugriffskontrolliste (ACL)
Verwenden von Gruppendokumenten
Erstellen einer Gruppe

### Verwenden der Selbstregistrierung

Der Sametime Server umfaßt eine Funktion zur Selbstregistrierung. Diese Funktion wird unterstützt, wenn Sametime in einer reinen Web-Umgebung installiert ist. Sie ist nicht verfügbar für die Installation von Sametime in einer Domino Umgebung.

Selbstregistrierung kann für einige Unternehmen ein Sicherheitsrisiko darstellen. Selbstregistrierung erlaubt jedem anonymen Benutzer, der mit einem Web-Browser auf den Server zugreift, sein eigenes Personendokument mit einem Internet-Kennwort im Adreßbuch anzulegen. Danach kann der Benutzer auf Sametime Connect zugreifen, um Chats mit anderen Mitgliedern der Sametime Community zu halten, und erhält Zugang zu geschützten Bereichen des Servers. Wenn ein solcher Zugriff ein Sicherheitsrisiko für Ihr Unternehmen bedeutet, schalten Sie die Funktion zur Selbstregistrierung aus.

Wenn Selbstregistrierung gestattet ist, sollten Besprechungsverwalter den Zugriff auf ihre Besprechungen einschränken, damit keine unerwünschten Benutzer daran teilnehmen können. Hierfür gibt der Besprechungsverwalter beim Anlegen der Besprechung ein Kennwort an oder gibt Namen in das Feld "Besprechung auf folgende Teilnehmer beschränken" auf dem Formular "Neue Besprechung" ein.

**Hinweis** Das Sametime Adreßbuch muß den Dateinamen NAMES.NSF besitzen, damit die Selbstregistrierung reibungslos funktioniert.

**Ein- und Ausschalten der Selbstregistrierung**

Die Funktion "Selbstregistrierung" steht nur Benutzern zur Verfügung, die über einen Web-Browser auf den Sametime Server zugreifen. Sametime muß hierfür in einer reinen Web-Umgebung installiert sein. Lotus Notes Benutzer können keine Selbstregistrierung durchführen.

Um die Selbstregistrierung ein- oder auszuschalten, gehen Sie wie folgt vor:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und dann "Netzwerk und Sicherheit".
2. Um Selbstregistrierung zu erlauben, markieren Sie das Feld "Benutzern erlauben, sich selbst im Sametime Adreßbuch zu registrieren".

   Um Selbstregistrierung auszuschalten, entfernen Sie die Markierung aus dem Feld "Benutzern erlauben, sich selbst im Sametime Adreßbuch zu registrieren".
3. Sie müssen auf die Schaltfläche "Aktualisieren" klicken und den Server neu starten, damit diese Änderung wirksam wird.

Wenn die Selbstregistrierung ausgeschaltet ist und ein Benutzer versucht, sich selbst zu registrieren, teilt ihm eine Meldung mit, daß dies nicht erlaubt ist.

Verwandte Themen anzeigen
Ein- und Ausschalten der Selbstregistrierung
Einführung in Sametime Sicherheit

## Ändern der Administrator-ECL für Lotus Notes R5 Clients

Dieses Thema betrifft Sie nur, wenn Sie Sametime in einer Domino R5-Umgebung installiert haben.

Die Ausführungskontrolliste (ECL) eines Administrators enthält in einem Adreßbuch auf einem Domino R5 Server ECL-Einstellungen für Java-Applet-Sicherheit. Wenn Benutzer auf den Sametime 1.5 Server mit Lotus Notes R5 Clients zugreifen, sollte der Administrator die ECL für Java-Applet-Sicherheit im Adreßbuch auf einem Domino R5 Server ändern.

Durch Ändern der ECL verhindern Sie, daß Notes R5 Benutzer beim ersten Teilnahmeversuch an einer aktiven Live-Sitzung über einen Notes R5 Client einen Sicherheitsalarm erhalten. Schrittweise Anleitungen finden Sie unter Ändern der Administrator-ECL für Notes R5 Clients.

Bei Installation und Setup eines Notes R5 Clients übernimmt der Client die ECL-Einstellungen aus der Administrator-ECL im Adreßbuch vom lokalen Server des Clients. Der Administrator sollte beim Aktualisieren der ECL für Java-Applet-Sicherheit folgendes beachten:

- Benutzer, die den R5 Client vor Ihrer Änderung der Administrator-ECL im Adreßbuch installiert haben, erhalten beim ersten Teilnahmeversuch an einer Sametime Besprechung einen Sicherheitsalarm. Diese Benutzer sollten im Warnungsfenster auf "Vertrauenswürdig" klicken.
- Benutzer, die den R5 Client nach Ihrer Änderung der Administrator-ECL installiert haben, erhalten den Sicherheitsalarm nicht und können ohne Störung an der Sametime Besprechung teilnehmen.

Verwandte Themen anzeigen
Details: Info über das Ändern der Administrator-ECL für Lotus Notes R5 Clients
Ändern der Administrator-ECL für Notes R5 Clients
Einführung in Sametime Sicherheit

## Details: Info über das Ändern der Administrator-ECL für Lotus Notes R5 Clients

Wenn ein Benutzer an einer Sametime Besprechung teilnimmt, werden Java-Applets vom Sametime Server zum Lotus Notes R5 Client auf dem lokalen Computer des Benutzers heruntergeladen. Die Java-Applets auf dem Client-Computer müssen eine Rückverbindung zum Sametime Server aufbauen, damit der Benutzer an einer Sametime Besprechung teilnehmen kann.

Die heruntergeladenen Java-Applets werden durch die Sametime Development/Lotus Notes Companion Products ID signiert. Damit die Java-Applets eine Verbindung zum Sametime Server aufbauen können, muß für die Sametime Development/Lotus Notes Companion Products ID "Zugriff auf Netzwerkadressen" in der ECL für Java-Applet-Sicherheit auf dem Notes R5 Client erlaubt sein.

Ist für die Sametime Development/Lotus Notes Companion Products ID "Zugriff auf Netzwerkadressen" in der ECL nicht gestattet, erhält der Client den Sicherheitsalarm. Die Wahl von "Vertrauenswürdig" aktualisiert die ECL auf dem Notes Client automatisch und ermöglicht dem Client, die Verbindung zur Sametime Besprechung aufzubauen.

Verwandte Themen anzeigen
Ändern der Administrator-ECL für Lotus Notes R5 Clients

## Ändern der Administrator-ECL für Notes R5 Clients

Der Administrator ändert die Administrator-ECL, damit Notes R5 Clients keine Sicherheitsalarme erhalten.

Um die Administrator-ECL zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das öffentliche Adreßbuch.
2. Wählen Sie "Actions - Edit Administration ECL".
3. Wählen Sie "Java Applet Security".
4. Klicken Sie auf "Add", und geben Sie "Sametime Development/Lotus Notes Companion Products" ein. Klicken Sie auf OK.

   **Hinweis** Sie können auch "*/Lotus Notes Companion Products" eingeben.
5. Markieren Sie "Sametime/Lotus Notes Companion Products", und wählen Sie "Access to network addresses" in der Spalte "Allow".
6. Stellen Sie sicher, daß "Allow user to modify" am oberen Ende des Dialogfelds "Execution Control List" aktiviert ist.
7. Klicken Sie auf OK.

Verwandte Themen anzeigen
Ändern der Administrator-ECL für Lotus Notes R5 Clients
Einführung in Sametime Sicherheit

## Internet- und Intranet-Sicherheit

Für die Teilnahme an Online-Besprechungen und Chat-Sitzungen über das Internet und Intranet müssen Sie Sicherheitsvorkehrungen treffen, um Ihr Netzwerk vor dem Risiko unbefugter Zugriffe zu schützen. Sametime bietet die folgenden Sicherheitsfunktionen, damit Sie diese Risiken minimieren können:

- Benutzeridentifizierung und -authentifizierung
- Zugriffskontrollisten für alle Datenbanken und Anwendungen auf dem Sametime Server
- Authentifizierung aller Verbindungen zu Services für Besprechungen und Community Services
- Verschlüsselung von Netzwerkdaten
- Kennwortschutz für Sametime Connect-Sitzungen

- Kennwortschutz für Online-Besprechungen
- Unterstützung des Secure Sockets Layer (SSL)-Protokolls

Wenn Ihr Unternehmen eine Firewall installiert hat, um Ihr Intranet vor unbefugtem externen Zugriff zu schützen, müssen Sie evtl. einen Sametime Server außerhalb der Firewall einsetzen und mit einem Sametime Server innerhalb der Firewall verbinden. Dieses Setup gestattet Benutzern außerhalb Ihrer Firewall, an Online-Besprechungen teilzunehmen, die auf einem Sametime Server innerhalb Ihrer Firewall gestartet wurden. Weitere Informationen finden Sie unter Verbinden von Sametime Servern.

Verwandte Themen anzeigen
Maximierung von Internet- und Intranet-Sicherheit für den Sametime Server

## Maximierung von Internet- und Intranet-Sicherheit für den Sametime Server

Zur Maximierung der Sicherheit für den Sametime Server sollten Sie:

- Server und Workstations physisch sichern,
- Firewalls einrichten, um den Zugriff externer Benutzer auf Ihr System zu verhindern,
- das Secure Sockets Layer (SSL)-Protokoll auf dem Sametime Server einrichten, um Internet- und Intranet-Benutzer und -Server zu authentifizieren,
- Datenbank-Zugriffskontrollisten (ACLs) definieren, um festzulegen, welche Benutzer und Server auf die Datenbank zugreifen können,
- ACLs für Datenbankkomponenten definieren, um festzulegen, welche Benutzer auf bestimmte Ansichten, Ordner, Formulare, Dokumente und Felder der Datenbank zugreifen können,
- lokale Datenbanken verschlüsseln,
- Netzwerkverkehr verschlüsseln,
- Kennwörter für Online-Besprechungen verwenden.

Verwandte Themen anzeigen
Internet- und Intranet-Sicherheit

## Physische Sicherheit für Server

Wenn der Sametime Server nicht physisch sicher ist, könnten unbefugte Benutzer Sicherheitsfunktionen umgehen, auf Datenbanken auf dem Server zugreifen, über das Betriebssystem Dateien kopieren oder löschen oder die Server-Hardware physisch beschädigen.

Um die physische Sicherheit des Sametime Servers zu gewährleisten, ergreifen Sie eine oder mehrere der folgenden Maßnahmen:

- Stellen Sie den Sametime Server in einer klimatisierten, sicheren Umgebung auf.
- Verwenden Sie den Server ohne Maus, und sperren Sie die Tastatur.
- Schützen Sie die Server-ID durch ein Kennwort. Starten Sie anschließend den Server manuell neu. Hierfür ist die Eingabe des Server-Kennwortes erforderlich.
- Verwenden Sie den Befehl "Server sichern", um die Konsole mit Kennwort zu schützen und die möglichen Aktionen einzuschränken, während der Server läuft.
- Legen Sie für Windows NT-Server einen Zugriffsschutz auf Dateien und Verzeichnisse fest, belegen Sie das Windows NT-Login-Konto mit Kennwortschutz, und sperren Sie die Windows NT-Konsole mit dem Kennwort des Login-Kontos.

Verwandte Themen anzeigen
Internet- und Intranet-Sicherheit

## Benutzeridentifizierung und -authentifizierung

Identifizierung und Authentifizierung sind ein Prozeß, bei dem der Name des Benutzers angegeben und überprüft wird, ob die Benutzerangaben korrekt sind. Sie können den Sametime Server so einrichten, daß Identifizierung und Authentifizierung von Benutzern verlangt wird oder daß anonymer Benutzerzugriff erlaubt ist. Anonymer Zugriff wird nur für Intranet-Zugriff empfohlen.

Internet- und Intranet-Zugriff auf den Sametime Server hängen davon ab, ob der Server den TCP/IP-Anschluß oder den Secure Sockets Layer (SSL)-Anschluß verwendet. Bei Installation und Setup wird der Sametime Server für den TCP/IP-Anschluß konfiguriert.

Sie können den TCP/IP-Anschluß für grundlegende Kennwortauthentifizierung einrichten, um Benutzer zu identifizieren und zu authentifizieren. Wenn der TCP/IP-Anschluß anonymen Benutzerzugriff erlaubt, kann jeder Benutzer auf den Server zugreifen, ohne identifiziert oder authentifiziert zu werden.

SSL bietet die höchste Sicherheitsstufe, ist jedoch am schwierigsten zu implementieren. Sie können den SSL-Anschluß für die Verwendung von SSL-Zertifikaten oder grundlegende Kennwortauthentifizierung einrichten, um Benutzer zu identifizieren oder zu authentifizieren. Wenn der SSL-Anschluß auf anonymen Benutzerzugriff eingestellt ist, wird der Server authentifiziert, aber Benutzer, die auf ihn zugreifen, werden weder identifiziert noch authentifiziert.

Verwandte Themen anzeigen
Anonymer Zugriff mit dem TCP/IP-Protokoll
Grundlegende Kennwortauthentifizierung mit dem TCP/IP-Protokoll
Secure Sockets Layer- (SSL) Protokoll

## Sicherheit in TCP/IP-Verbindungen

Web-Browser kommunizieren mit Hilfe des HTTP-Protokolls über den TCP/IP-Anschluß mit dem Sametime Server. Die über TCP/IP-Verbindungen übertragenen Daten sind reiner Text. Folgende Konfigurationseinstellungen steuern Internet- und Intranet-Sicherheit auf dem Sametime Server über TCP/IP-Verbindungen:

- Die Einstellungen unter "Internet-Anschluß und Sicherheitskonfiguration" im Serverdokument
- Die Zugriffskontrolliste (ACL) jeder Datenbank
- Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" jeder Datenbank-ACL

Die TCP/IP-Konfigurationseinstellungen finden Sie unter "Internet-Anschluß und Sicherheitskonfiguration" im Serverdokument. Folgende Tabelle beschreibt die Einstellungen, die Sie für jedes aktivierte Internet-Protokoll angeben.

| TCP/IP-Einstellung | Beschreibung |
|---|---|
| TCP/IP-Anschlußnummer | Gibt den TCP/IP-Anschluß an. Standard für das HTTP-Protokoll ist Anschluß 80. |
| TCP/IP-Anschlußstatus | Aktiviert oder deaktiviert den TCP/IP-Anschluß. |
| Authentifizierungs-optionen | Legen fest, ob der Server anonymen Benutzerzugriff erlaubt oder grundlegende Kennwortauthentifizierung verlangt, um Benutzer zu identifizieren oder zu authentifizieren. Sie können jedes Internet-Kommunikationsprotokoll separat konfigurieren. Sie können z. B. anonyme HTTP-Verbindungen gestatten, aber für LDAP-Verbindungen einen Benutzernamen und ein Kennwort verlangen. |

Bei Installation und Setup des Sametime Servers werden die TCP/IP-Authentifizierungsoptionen für HTTP so eingestellt, daß sie anonymen Zugriff sowie grundlegende Kennwortauthentifizierung gestatten. Wenn beide Authentifizierungsoptionen aktiviert sind, können Sie einige Datenbanken für anonymen Zugriff einrichten und für andere Datenbanken grundlegende Kennwortauthentifizierung verlangen. Beispielsweise können alle Benutzer anonym auf die Seite "Willkommen bei Sametime" (STCenter.nsf) zugreifen, für das Sametime Online-Besprechungszentrum müssen sie jedoch ein Kennwort eingeben.

Die Datenbank-ACL definiert Benutzerzugriff auf den Inhalt der Datenbank. Sie listet jeden Benutzer und jede Benutzergruppe mit der jeweiligen Zugriffsebene auf. Sie können in der Datenbank-ACL auch die Datenbankzugriffsebene für anonyme Benutzer festlegen.

Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" jeder Datenbank-ACL gibt die maximale Zugriffsebene auf die Datenbank durch Web-Browser-Clients an. Diese Einstellung hat Vorrang vor den einzelnen Ebenen, die in der ACL festgelegt sind.

**Hinweis** Sie können auch Daten verschlüsseln, die bei Online-Besprechungen gesendet werden.

Verwandte Themen anzeigen
Anonymer Zugriff mit dem TCP/IP-Protokoll
Gestatten anonymen Serverzugriffs für Browser-Clients über TCP/IP
Grundlegende Kennwortauthentifizierung mit dem TCP/IP-Protokoll

## Anonymer Zugriff mit dem TCP/IP-Protokoll

Anonymer Zugriff mit dem TCP/IP-Protokoll zeigt folgende Charakteristiken:

- Benutzer werden beim Zugriff auf Datenbanken oder Anwendungen auf dem Server nicht identifiziert oder authentifiziert.
- Zwischen Benutzer und Sametime Server übertragene Daten werden nicht verschlüsselt.
- Anonyme Benutzer werden in den Wartungsprotokolldateien nicht identifiziert. Sämtliche Aktivitäten anonymer Benutzer werden unter dem Namen "Anonym" aufgezeichnet.
- Anonyme Benutzer können im Online-Besprechungszentrum Online-Besprechungen starten, ändern und an ihnen teilnehmen.

Die anonyme Zugriffsebene verlangt die wenigste Wartung vom Administrator, ist aber auch die unsicherste. Sie sollten anonymen Zugriff gestatten, wenn Sie die Identität von Benutzern, die auf Ihren Server zugreifen, nicht kennen müssen. Verwenden Sie z. B. anonymen Zugriff, wenn sich der Sametime Server hinter Ihrer Firewall befindet und Sie nur bewährten Intranet-Benutzern den Zugriff gestatten wollen.

Verwandte Themen anzeigen
Gestatten anonymen Serverzugriffs für Browser-Clients über TCP/IP

## Gestatten anonymen Serverzugriffs für Browser-Clients über TCP/IP

Führen Sie nachstehende Schritte aus, um Benutzern anonymen Zugriff auf den Server zu erlauben. Der Server ist standardmäßig auf anonymen Zugriff eingestellt.

1. Erstellen Sie den Eintrag "Anonym" in den Zugriffskontrollisten (ACLs) von Datenbanken auf dem Server, und weisen Sie die geeignete Zugriffsebene zu, in der Regel Leserzugriff.

   **Hinweis** Datenbank-ACLs ohne den Eintrag "Anonym" weisen anonymen Benutzern und Servern den Standardzugriff zu.
2. Klicken Sie im Sametime Administrationswerkzeug auf "Server" und anschließend auf "Server".
3. Wählen Sie den Namen des Sametime Servers aus, um das Serverdokument zu öffnen.
4. Wählen Sie in den TCP/IP-Authentifizierungsoptionen im Bereich "Internet-Anschluß und Sicherheitskonfiguration" die Option "Ja" im Feld "Anonym" in der Spalte für das HTTP-Protokoll.
5. Richten Sie die Datenbank-ACL für den Zugriff anonymer Benutzer ein.
6. Speichern Sie das Dokument.
7. Beenden Sie den Server, und starten Sie ihn neu, damit die Änderungen wirksam sind.

Verwandte Themen anzeigen
Anonymer Zugriff mit dem TCP/IP-Protokoll
Grundlegende Kennwortauthentifizierung mit dem TCP/IP-Protokoll

### Details: Gestatten anonymen Serverzugriffs

- Wenn der Administrator keinen anonymen Zugriff erlaubt, erhalten alle anonymen Internet- und Intranet-Benutzer beim Zugriff auf den Server eine entsprechende Meldung. Wenn Sie grundlegende Kennwortauthentifizierung auf dem Server einrichten, müssen Benutzer einen Benutzernamen und ein Kennwort eingeben, bevor diese Meldung erscheint. Die Einstellung "Anonym" im Serverdokument setzt individuelle Datenbankzugriffskontrollen für anonyme Benutzer außer Kraft.
- Wenn "Name & Kennwort" sowie "Anonym" für ein Internet-Protokoll aktiviert sind und Sie in der Datenbank-Zugriffskontrolliste (ACL) anonymen Zugriff gestatten, erfolgt die Verbindung der Benutzer mit anonymem Zugriff. Der Server fordert vom Benutzer keinen Namen und kein Kennwort, selbst wenn der Benutzer für grundlegende Kennwortauthentifizierung eingerichtet ist.

### Grundlegende Kennwortauthentifizierung mit dem TCP/IP-Protokoll

Grundlegende Kennwortauthentifizierung mit dem TCP/IP-Protokoll hat folgende Charakteristiken:

- Benutzer werden beim Zugriff auf Datenbanken und Anwendungen auf dem Server identifiziert oder authentifiziert.
- Nur beim Server bekannte Benutzer können auf seine Anwendungen oder Datenbanken zugreifen.
- Internet- und Intranet-Benutzer müssen über ein Internet-Kennwort verfügen, das in ihrem Personendokument gespeichert ist, um auf Server-Anwendungen und -Datenbanken zuzugreifen.
- Daten, die zwischen Benutzer und Sametime Server übertragen werden (einschließlich Name und Kennwort), werden nicht verschlüsselt.
- Benutzer werden in den Wartungsprotokolldateien identifiziert.
- Die Zugriffskontrolliste (ACL) des Online-Besprechungszentrums definiert, welche Benutzer Online-Besprechungen starten, ändern und an ihnen teilnehmen können.

Wenn die grundlegende Kennwortauthentifizierung aktiviert ist, werden Browser-Clients, die über TCP/IP auf den Sametime Server zugreifen, nur dann authentifiziert, wenn sie versuchen, eine eingeschränkte Aktion auszuführen, z. B. eine Datenbank zu öffnen, die keinen anonymen Zugriff erlaubt. Der Sametime Server fordert den Benutzer auf, einen gültigen Namen und ein gültiges Kennwort einzugeben, und prüft dann, ob diese Angaben mit der Information im Personendokument des Benutzers im Adreßbuch übereinstimmen. Die Authentifizierung ist erfolgreich, wenn der Benutzername und das Kennwort gültig sind und der Benutzer einzeln oder als Mitglied einer Gruppe in der Datenbank-ACL aufgeführt ist.

Grundlegende Kennwortauthentifizierung identifiziert Benutzer, hindert jedoch unbefugte Benutzer nicht daran, Netzwerkübertragungen zu "belauschen" oder Server-Zugang zu erhalten, indem sie das Kennwort erraten.

Verwandte Themen anzeigen
Anonymer Zugriff mit dem TCP/IP-Protokoll
Gestatten anonymen Serverzugriffs für Browser-Clients über TCP/IP

### Namen und Kennwort von Internet- und Intranet-Clients verlangen

Führen Sie die folgenden Schritte aus, um von Benutzern einen Namen und ein Kennwort für den Zugriff auf den Server zu verlangen:

1. Klicken Sie im Sametime Administrationswerkzeug auf "Server" und anschließend auf "Server".
2. Wählen Sie den Namen des Sametime Servers aus, um das Serverdokument zu öffnen.
3. Wählen Sie in den TCP/IP-Authentifizierungsoptionen im Bereich "Internet-Anschluß und Sicherheitskonfiguration" die Option "Ja" im Feld "Name und Kennwort" in der Spalte für das HTTP-Protokoll.
4. Speichern Sie das Dokument.
5. Richten Sie die Datenbank-Zugriffskontrolliste (ACL) ein.

**Hinweis** Sie müssen ein Personendokument anlegen, das für jeden Benutzer ein Internet-Kennwort enthält.

### Details: Name und Kennwort von Internet- und Intranet-Clients verlangen

- Wenn Sie neue Personendokumente mit Hilfe eines Lotus Notes Clients anlegen, verschlüsselt Notes das Internet-Kennwortfeld mit der vorherigen Version des Kennwortformats. Verwenden Sie dieses Format, wenn Benutzer auf Server zugreifen, die eine Vorgängerversion von Sametime verwenden. Für automatische Verwendung des neuen Kennwortformats können Sie einen Agent erstellen, der alle neuen Dokumente in der Datenbank abarbeitet und automatisch das Kennwort zum neuen Format aktualisiert.
- Der Befehl "&Login" zwingt Benutzer, einen Namen und ein Kennwort anzugeben, und verhindert den standardmäßig eingestellten anonymen Zugriff. Sie können "&Login" als Argument an einen URL-Befehl anfügen, z. B. an OpenDatabase, OpenView und OpenDocument. Andernfalls erhalten Benutzer anonymen Zugriff.
- Wenn "Name & Kennwort" sowie "Anonym" im TCP/IP-Abschnitt aktiviert sind und Sie anonymen Zugriff gestatten, erfolgt die Verbindung zwischen Server und Benutzer mit anonymem Zugriff. Wenn "Name & Kennwort" und "Anonym" im TCP/IP-Abschnitt aktiviert sind und anonymer Zugriff auf die Datenbank nicht erlaubt ist, fordert der Server den Benutzer zur Eingabe eines Namens und eines Kennwortes auf.

### Datenbank-Zugriffskontrollisten (ACLs)

Jede Datenbank auf dem Sametime Server verfügt über eine Zugriffskontrolliste (ACL), die den Benutzerzugriff auf die Datenbank steuert. Die Datenbank-ACL listet alle Benutzer und Gruppen mit ihrer jeweiligen Zugriffsebene auf. Benutzer und Gruppen, die nicht explizit aufgeführt sind, erhalten die Standard-Zugriffsebene. Jeder ACL-Eintrag gibt einen Benutzertyp, eine Zugriffsebene, eine zugehörige Autorisierung und optional zugewiesene Funktionen an.

#### Benutzertypen

Der Benutzertyp bezeichnet den Benutzer als Person, Server oder Gruppe. Folgende Benutzertypen sind möglich: Unbestimmt, Person, Server, Personengruppe, Servergruppe oder Gemischte Gruppe. Der Benutzertyp unterscheidet zwischen zwei unterschiedlichen Benutzertypen mit demselben Namen.

**Hinweis** Wenn Sie Sametime als reinen Web-Server einsetzen, werden Servernamen nicht in Datenbank-ACLs aufgelistet.

#### Gruppendokumente

Gruppendokumente vereinfachen die ACL-Administration, da Sie an zentraler Stelle Mitglieder mit den gleichen Zugriffsebenen verwalten und diese nicht mehr einzeln mehreren Datenbanken hinzufügen müssen. Sie können ein Gruppendokument im Adreßbuch anlegen, das Mitglieder mit derselben Zugriffsebene enthält, und dann diese Gruppe einer oder mehreren Datenbank-ACLs hinzufügen.

#### Einstellungen für "Internet-Anschluß und Sicherheitskonfiguration"

Sie müssen die Einstellungen im Abschnitt "Internet-Anschluß und Sicherheitskonfiguration" des Serverdokuments konfigurieren, damit die Datenbank-ACLs wirksam werden. Diese Einstellungen beeinflussen Einträge in der ACL. Wenn z. B. die Internet-Anschluß- und Sicherheitseinstellungen anonymen Zugriff auf den Server gestatten, kann der Administrator in einer Datenbank-ACL den Eintrag "Anonym" anlegen und eine Zugriffsebene zuweisen. Alle anonymen Benutzer können dann in der Datenbank Aktionen ausführen, die die zugewiesene Zugriffsebene erlaubt.

Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" jeder Datenbank-ACL gibt die maximale Zugriffsebene auf die Datenbank für Web-Browser-Clients an. Diese Einstellung setzt einzelne Ebenen außer Kraft, die in der ACL angegeben sind.

**Hinweis** Der Sametime Server zeichnet alle Änderungen an der ACL in der Notes-Protokolldatei auf.

Verwandte Themen anzeigen
ACL-Zugriffsebenen
Zugriffskontrollisten- (ACL-) Autorisierungen
Funktionen in Zugriffskontrollisten (ACLs)

## ACL-Zugriffsebenen

Datenbank-Zugriffskontrollisten (ACLs) definieren Zugriffsebenen für Benutzer und steuern damit, welche Aktionen ein Benutzer am Inhalt einer Datenbank und an der Datenbank selbst vornehmen kann. Zugriffsebenen reichen von "Kein Zugriff", die einen Benutzer daran hindert, eine Datenbank zu öffnen, bis zu "Manager", die ihm gestattet, die ACL und alle Dokumente in der Datenbank zu lesen, anzulegen und zu bearbeiten.

Benutzer, die sowohl einzeln als auch als Gruppenmitglieder in der ACL aufgeführt sind, können über unterschiedliche Zugriffsebenen verfügen. Die Zugriffsebene für einen Einzeleintrag hat Vorrang vor der Zugriffsebene für einen Gruppeneintrag. Wenn ein Benutzer mehreren Gruppen angehört, erhält er die höchste Zugriffsebene, die einer dieser Gruppen zugewiesen ist. Wenn ein Benutzer oder eine Gruppe über eine einzelne Zugriffsebene in der ACL und eine andere Zugriffsebene in einem Datenbankdokument verfügt, wie z. B. Lesen oder Anzeigen der Zugriffsliste, hat die Zugriffsebene der Datenbankkomponente Vorrang vor der Zugriffsebene des Benutzers bzw. der Gruppe.

Nachstehend sind die Zugriffsebenen von der niedrigsten zur höchsten aufgeführt. Eine höhere Zugriffsebene verfügt über alle Autorisierungen, die niedrigeren Zugriffsebenen zugewiesen sind. Autoren können z. B. alle Funktionen eines Archivars und eines Lesers ausführen.

**Kein Zugriff**

Der Benutzer kann nicht auf die Datenbank zugreifen. Wenn Sie dies als Standardzugriff für eine Datenbank einstellen, kann nur ein Benutzer auf die Datenbank zugreifen, der über ein Personendokument im Adreßbuch verfügt und in der ACL aufgelistet ist.

**Archivar**

Der Benutzer kann Dokumente anlegen, jedoch keine Dokumente in der Datenbank ansehen, auch nicht die von ihm erstellten. Diese Zugriffsebene wird im allgemeinen nicht für Sametime Datenbanken verwendet.

**Leser**

Der Benutzer kann Dokumente in einer Datenbank lesen, aber nicht anlegen oder bearbeiten. Sie sollten z. B. in der ACL des Online-Besprechungszentrums Benutzern den Leserzugriff zuweisen, die an Besprechungen teilnehmen, jedoch keine Besprechungen starten dürfen. Gewähren Sie in einer Diskussions-Datenbank-ACL Benutzern Leserzugriff, wenn diese Diskussionsdokumente lesen, aber keine Diskussionsthemen erstellen oder beantworten dürfen.

**Autor**

Der Benutzer darf Dokumente anlegen und von ihm erstellte Dokumente bearbeiten. Er kann keine Dokumente bearbeiten, die andere Benutzer angelegt haben. Weisen Sie in der ACL des Online-Besprechungszentrums Benutzern den Autorenzugriff zu, wenn diese Besprechungen anlegen dürfen. Der Benutzer kann von ihm angelegte Besprechungen ändern, jedoch keine von anderen Benutzern erstellten Besprechungen. Gewähren Sie in einer Diskussions-Datenbank-ACL Benutzern Autorenzugriff, wenn diese Diskussionsthemen starten und beantworten dürfen. Ein Diskussionsdatenbank-Benutzer mit Autorenzugriff kann nur die Diskussionsdokumente bearbeiten, die er selbst erstellt hat.

**Editor**

Der Benutzer kann alle Dokumente in der Datenbank lesen, anlegen und bearbeiten, auch von anderen Benutzern angelegte Dokumente. Weisen Sie in der ACL des Online-Besprechungszentrums den Benutzern Editorzugriff zu, die von anderen Benutzern erstellte Online-Besprechungen bearbeiten dürfen. Weisen Sie im Adreßbuch einem Administrator den Editorzugriff zu, der für das Anlegen und Führen von Personendokumenten im öffentlichen Adreßbuch verantwortlich ist.

**Entwickler**

Der Benutzer kann Volltextindizes erstellen, alle Designelemente der Datenbank ändern sowie alle Dokumente in der Datenbank lesen, anlegen und bearbeiten. Diese Zugriffsebene ist in erster Linie für Unternehmen gedacht, die den Sametime Server in einer Lotus Domino Umgebung einsetzen.

**Manager**

Der Benutzer kann die ACL und alle Dokumente in der Datenbank lesen, erstellen und bearbeiten, ACL-Einstellungen ändern und die Datenbank löschen. Keine andere Zugriffsebene gestattet das Ändern der ACL und das Löschen von Datenbanken. Diese Zugriffsebene erhalten gewöhnlich Sametime Administratoren.

Für jede Datenbank muß mindestens ein Manager vorhanden sein. Sie sollten zwei Personen den Managerzugriff gewähren, für den Fall, daß ein Manager abwesend oder nicht verfügbar ist. Der Manager hat Zugriff auf das Adreßbuch und das Sametime Administrationswerkzeug. Der Managerzugriff kann auch alle Aktionen ausführen, die niedrigere Zugriffsebenen gestatten.

Verwandte Themen anzeigen
Zugriffskontrollisten- (ACL-) Autorisierungen
Funktionen in Zugriffskontrollisten (ACLs)

## Zugriffskontrollisten- (ACL-) Autorisierungen

Die Datenbank-Zugriffskontrolliste (ACL) definiert Autorisierungen für Benutzer. Je nach Zugriffsebene werden einem Benutzer einige ACL-Autorisierungen zugeteilt oder verweigert oder sind optional. Die folgenden Autorisierungen sind in der ACL aufgelistet:

**Dokumente erstellen**

Diese Autorisierung ist Managern, Entwicklern, Editoren und Archivaren permanent zugeteilt, Lesern permanent verweigert, Autoren optional zugeteilt.

**Dokumente löschen**

Diese Autorisierung ist Lesern und Archivaren permanent verweigert, Managern, Entwicklern, Editoren und Autoren optional zugeteilt.

**Persönliche Agents erstellen**

Diese Autorisierung ist Managern und Entwicklern permanent zugeteilt, Editoren, Autoren und Lesern optional zugeteilt.

Deaktivieren Sie diese Autorisierung auf Server-Datenbanken, um bestimmte Benutzer daran zu hindern, persönliche Agents zu erstellen, die Plattenspeicher und Verarbeitungszeit auf dem Server in Anspruch nehmen. Hindern Sie mit Hilfe des Abschnitts "Agent Manager Restrictions" im Serverdokument des Adreßbuchs Benutzer daran, persönliche Agents auf einem Server auszuführen, selbst wenn die Autorisierung "Persönliche Agents erstellen" in einer Server-Datenbank-ACL aktiviert ist.

**Persönliche Ordner/Ansichten erstellen**

Diese Autorisierung ist Managern und Entwicklern permanent zugeteilt, Archivaren permanent verweigert und Editoren, Autoren und Lesern optional zugeteilt.

Persönliche Ordner und Ansichten, die auf einem Server erstellt werden, sind sicherer und stehen auf mehreren Servern zur Verfügung. Administrative Agents können nur Ordner und Ansichten beeinflussen, die auf einem Server gespeichert sind. Wenn diese Autorisierung deaktiviert ist, können Benutzer dennoch persönliche Ordner und Ansichten anlegen, die auf ihren lokalen Workstations gespeichert sind. Deaktivieren Sie diese Autorisierung, um Speicherplatz auf einem Server zu sparen.

**Gemeinsame Ordner/Ansichten erstellen**

Diese Autorisierung ist Managern und Entwicklern permanent zugeteilt, Autoren, Lesern und Archivaren permanent verweigert und Editoren optional zugeteilt.

Verweigern Sie Editoren diese Autorisierung, um Plattenplatz auf einem Server zu sparen und eine bessere Kontrolle über das Datenbankdesign zu behalten.

**LotusScript erstellen**

Diese Autorisierung ist Managern, Entwicklern, Editoren, Autoren und Lesern permanent zugeteilt und Archivaren verweigert. Die Autorisierung gilt nur für einen Sametime Server, der in einer Domino Umgebung installiert ist.

Deaktivieren Sie diese Autorisierung auf Server-Datenbanken, damit bestimmte Benutzer keine eingeschränkten und uneingeschränkten LotusScript® Agents ausführen können, die Plattenplatz und Verarbeitungszeit auf dem Server beanspruchen. Hindern Sie mit Hilfe des Abschnitts "Agent Manager Restrictions" im Serverdokument des Adreßbuchs Benutzer daran, eingeschränkte oder uneingeschränkte LotusScript Agents auf einem Server auszuführen, auch wenn die Autorisierung "Persönliche Agents erstellen" in einer Server-Datenbank-ACL aktiviert ist.

**Öffentliche Dokumente lesen**

Diese Autorisierung ist Managern, Entwicklern, Editoren, Autoren und Lesern permanent zugeteilt, Archivaren jedoch nur optional zugeteilt.

**Öffentliche Dokumente schreiben**

Diese Autorisierung ist Managern, Entwicklern und Editoren permanent zugeteilt, aber Autoren, Lesern und Archivaren nur optional zugeteilt.

Öffentliche Dokumente sind einem breiten Web-Publikum zugänglich, wie z. B. die belegten und freien Termine in Ihrem persönlichen Kalender. Benutzer mit der Autorisierung "Öffentliche Dokumente schreiben" können öffentliche Dokumente in einer Datenbank lesen, erstellen, bearbeiten und löschen.

Benutzer ohne diese Autorisierung müssen ein Kennwort eingeben, wenn sie auf eine Datenbank mit öffentlichen Dokumenten zugreifen. Nach Eingabe des Benutzernamens und des Kennworts erhält der Benutzer die Standard-Zugriffsebene für die Datenbank.

**Hinweis** Nur die Autorisierungen "Lesen" bzw. "Öffentliche Dokumente schreiben" werden optional Benutzern zugeteilt, denen "Kein Zugriff" auf die Datenbank zugewiesen ist.

Verwandte Themen anzeigen
ACL-Zugriffsebenen
Funktionen in Zugriffskontrollisten (ACLs)

## Funktionen in Zugriffskontrollisten (ACLs)

Funktionen in Datenbank-Zugriffskontrollisten (ACLs) ermöglichen Zugriff auf individuelle Datenbankkomponenten, wie z. B. Formulare oder Ansichten. Mit Hilfe der ACL-Funktionen können Sie die Autorität zur Verwaltung bestimmter Dokumente in einer Datenbank delegieren. Sie können z. B. die Funktionen von UserCreator und UserModifier in der Adreßbuch-ACL dem Administrator zuteilen, der für das Anlegen und Führen von Personendokumenten verantwortlich ist.

ACL-Funktionen sind optional. Sie können sich auch für breitere Zugriffsebenen entscheiden und auf Funktionen verzichten.

**Hinweis** Sie können in einer Datenbank bis zu 75 Funktionen definieren.

Verwandte Themen anzeigen
Zugriffskontrollisten- (ACL-) Autorisierungen

## Verwalten von Zugriffskontrollisten

Die folgenden Verfahren erläutern, wie Sie die üblichen Aufgaben beim Verwalten von Zugriffskontrollisten (ACLs) erledigen:

- Anzeigen einer Datenbank-ACL
- Hinzufügen von Benutzern zu einer Datenbank-ACL
- Einrichten von anonymem Zugriff in einer Datenbank-ACL
- Einrichten der grundlegenden Kennwortauthentifizierung in einer Datenbank-ACL

Verwandte Themen anzeigen
Anzeigen einer Datenbank-Zugriffskontrolliste (ACL)
Hinzufügen von Benutzern zu einer Datenbank-Zugriffskontrolliste (ACL)

## Anzeigen einer Datenbank-Zugriffskontrolliste (ACL)

Eine Datenbank-Zugriffskontrolliste (ACL) anzeigen:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und anschließend "Datenbanksicherheit".
2. Wählen Sie eine Datenbank aus der Liste.
3. Klicken Sie auf "Zugriff".

Verwandte Themen anzeigen
Hinzufügen von Benutzern zu einer Datenbank-Zugriffskontrolliste (ACL)
Datenbank-Zugriffskontrollisten (ACLs)

## Hinzufügen von Benutzern zu einer Datenbank-Zugriffskontrolliste (ACL)

Benutzer in eine Datenbank-Zugriffskontrolliste (ACL) aufnehmen:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und anschließend "Datenbanksicherheit".
2. Wählen Sie eine Datenbank aus der Liste.
3. Klicken Sie auf "Zugriff".
4. Klicken Sie auf "Hinzufügen".
5. Geben Sie im Dialogfenster den Benutzernamen aus dem Personendokument, den Gruppennamen aus dem Gruppendokument oder den Servernamen aus dem Serverdokument ein, und klicken Sie auf OK.
6. Wählen Sie den Benutzernamen aus.
7. Wählen Sie im Feld "Benutzertyp" die Art des Benutzers aus ("Unbestimmt", "Person", "Server", "Personengruppe", "Servergruppe" oder "Gemischte Gruppe").
8. Weisen Sie dem Benutzer im Feld "Zugriff" eine Zugriffsebene zu ("Manager", "Entwickler", "Editor", "Autor", "Leser", "Archivar" oder "Kein Zugriff").
9. Bearbeiten Sie die Autorisierungen falls erforderlich.
10. Klicken Sie auf "Senden".

Verwandte Themen anzeigen
Anzeigen einer Datenbank-Zugriffskontrolliste (ACL)
Datenbank-Zugriffskontrollisten (ACLs)

## Einrichten von anonymem Zugriff in einer Datenbank-Zugriffskontrolliste (ACL)

Der Sametime Server muß entsprechend eingerichtet sein, damit Web-Browser-Clients anonym auf ihn zugreifen können. Gehen Sie wie folgt vor, um Benutzern anonymen Zugriff auf die Datenbank zu gewähren:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und anschließend "Datenbanksicherheit".
2. Wählen Sie eine Datenbank aus der Liste.
3. Klicken Sie auf "Erweitert".
4. Stellen Sie "Max. Internet-Namen- & Kennwortzugriff" auf "Manager", die höchste Zugriffsebene, ein.

   **Hinweis** Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" einer jeden Datenbank-Zugriffskontrolliste (ACL) gibt die maximale Zugriffsebene für Web-Browser-Clients an. Diese Einstellung setzt etwaige höhere individuelle Zugriffsebenen außer Kraft, die in der ACL eingestellt sind. Wenn Sie z. B. "Max. Internet-Namen- & Kennwortzugriff" einstellen und dem Eintrag "Anonym" in der Datenbank-ACL Managerzugriff zuweisen, erhalten anonyme Benutzer nur den Autorenzugriff auf die Datenbank. Wenn Sie andererseits "Max. Internet-Namen- & Kennwortzugriff" auf "Manager" einstellen und dem Eintrag "Anonym" in der Datenbank-ACL Leserzugriff zuweisen, erhalten anonyme Benutzer nur den Leserzugriff auf die Datenbank
5. Klicken Sie auf "Zugriff".
6. Wenn der Eintrag "Anonym" nicht existiert, legen Sie ihn wie folgt an:
   - Klicken Sie auf "Hinzufügen".
   - Geben Sie "Anonym" in das Dialogfenster ein, und klicken Sie auf OK.
7. Wählen Sie den Eintrag "Anonym" aus.
8. Weisen Sie im Feld "Zugriff" dem Eintrag "Anonym" eine Zugriffsebene zu (z. B. Autor).
9. Bearbeiten Sie die Standard-Autorisierungen falls erforderlich.
10. Klicken Sie auf "Senden".

    Verwandte Themen anzeigen
    
    Einrichten der grundlegenden Kennwortauthentifizierung in einer Datenbank-Zugriffskontrolliste (ACL)
    Datenbank-Zugriffskontrollisten (ACLs)

## Einrichten der grundlegenden Kennwortauthentifizierung in einer Datenbank-Zugriffskontrolliste (ACL)

Der Sametime Server muß so eingerichtet werden, daß er von Web-Browser-Clients beim Zugriff auf die Datenbank einen gültigen Namen und ein gültiges Kennwort verlangt. Gehen Sie hierfür wie folgt vor:

1. Wählen Sie im Sametime Administrationswerkzeug "Server" und anschließend "Datenbanksicherheit".
2. Wählen Sie die Datenbank aus der Liste.
3. Klicken Sie auf "Erweitert".
4. Stellen Sie "Max. Internet-Namen- & Kennwortzugriff" auf "Manager", die maximale Zugriffsebene, ein.

   **Hinweis** Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" jeder Datenbank-Zugriffskontrolliste (ACL) gibt die maximale Zugriffsebene für Web-Browser-Clients an. Diese Einstellung setzt etwaige höhere individuelle Zugriffsebenen außer Kraft, die in der ACL festgelegt sind. Wenn Sie z. B. "Max. Internet-Namen- & Kennwortzugriff" auf "Autor" einstellen und dem Eintrag "Anonym" in der Datenbank-ACL Managerzugriff zuweisen, erhalten anonyme Benutzer nur den Autorenzugriff auf die Datenbank. Wenn Sie andererseits "Max. Internet-Namen- & Kennwortzugriff" auf "Manager" einstellen und dem Eintrag "Anonym" in der Datenbank-ACL Leserzugriff zuweisen, erhalten anonyme Benutzer nur den Leserzugriff auf die Datenbank.
5. Klicken Sie auf "Zugriff".
6. Wenn der Eintrag "Anonym" nicht existiert, legen Sie ihn wie folgt an:
   - Klicken Sie auf "Hinzufügen".

- Geben Sie "Anonym" in das Dialogfenster ein, und klicken Sie auf OK.

7. Wählen Sie den Eintrag "Anonym" aus, und wählen Sie "Kein Zugriff" im Feld "Zugriff".
8. Wählen Sie den Eintrag "Standard" aus, und wählen Sie "Kein Zugriff" im Feld "Zugriff".
9. Klicken Sie auf die Schaltfläche "Hinzufügen", um Benutzernamen oder Gruppennamen in die ACL einzufügen. Klicken Sie nach dem Hinzufügen jedes Namens auf OK.
10. Wenn Sie alle gewünschten Benutzer und Gruppennamen hinzugefügt haben, klicken Sie auf "Senden".

Verwandte Themen anzeigen

Einrichten von anonymem Zugriff in einer Datenbank-Zugriffskontrolliste (ACL)
Datenbank-Zugriffskontrollisten (ACLs)

## Web-Benutzern die Anzeige einer Liste von Datenbanken auf dem Server gestatten

Mit Hilfe des Befehls "?OpenServer" können Sie steuern, ob Web-Benutzer eine Liste der Datenbanken auf dem Server anzeigen können.

1. Klicken Sie im Sametime Administrationswerkzeug auf "Server" und anschließend auf "Server".
2. Öffnen Sie das Serverdokument für diesen Server, und zeigen Sie den Abschnitt "Sicherheit" an.
3. Klicken Sie im Feld "Allow HTTP clients to browse databases" auf "Ja".

   **Hinweis** Wenn dieses Feld auf "Nein" eingestellt ist, haben Web-Benutzer keinen Zugriff auf eine Liste der Datenbanken; sie können aber dennoch Datenbanken öffnen, für die sie nicht zugriffsberechtigt sind.
4. Speichern Sie das Dokument.

## Authentifizieren von Verbindungen zum Sametime Server

Das Online-Besprechungszentrum, Sametime Connect und andere Sametime Anwendungen verlangen zusätzliche Verbindungen zwischen Client und Sametime Server. Der Sametime Server verwendet die Datenbanken "Secrets" (StAuthS.nsf) und "Tokens" (StAuthT.nsf), um Sametime Benutzer über diese zusätzlichen Verbindungen zu authentifizieren. Diese Datenbanken werden **nicht** zur Authentifizierung von Benutzern verwendet, wenn sie sich beim Sametime Server über den Sametime Connect Client, einen Web-Browser oder einen Notes Client anmelden. Der Sametime Server authentifiziert mit Hilfe dieser Datenbanken nur Datenverbindungen in einer Online-Besprechung sowie Benutzer, wenn diese ein Dokument in einer Sametime Anwendung mit Online- und Chat-Fähigkeiten öffnen.

Um die Sicherheit dieser zusätzlichen Verbindungen für einen Browser-Client zu maximieren, muß der Sametime Server Secure Sockets Layer- (SSL) Verbindungen zu Besprechungs- und Community Services verwenden. Für maximale Sicherheit dieser zusätzlichen Verbindungen für einen Notes Client muß der Sametime Server den Netzwerkverkehr verschlüsseln.

Wenn der Sametime Server auf SSL-Verbindungen oder Verschlüsselung des Netzwerkverkehrs von einem Notes Client eingestellt ist, werden die in einer Online-Besprechung oder einer Chat-Sitzung ausgetauschten Daten nicht verschlüsselt. Sie können beim Erstellen einer Online-Besprechung festlegen, daß ausgetauschte Daten verschlüsselt werden.

## Info über Firewalls

Eine Firewall steuert den Zugriff auf Ihr Netzwerk und schützt Ihr Intranet vor unbefugtem externem Internet-Zugriff. Firewalls werden häufig mit einem Proxy-Server eingesetzt und implementieren Sicherheitsmaßnahmen wie Paketfilter, Gateways auf Anwendungsebene und geschaltete Gateways. Ein Proxy-Server vermittelt Anforderungen zwischen Benutzern innerhalb Ihrer Firewall und Servern außerhalb Ihrer Firewall. Proxies maskieren die Absenderadresse des anfordernden Computers, um die Anonymität von Benutzern innerhalb Ihrer Firewall zu wahren.

Nachstehende Tabelle erläutert drei Arten von Firewall-Software- und Hardware-Konfigurationen.

| Firewall-Typ | Beschreibung |
|---|---|
| Paketfilter | Prüft, wohin ein Datenpaket übertragen wird und welche Informationsart es enthält. Wenn Ihre Netzwerkpolitik eine Übertragung zu diesem Zielort gestattet und die Informationsart für den Zugang bzw. das Verlassen Ihres Netzwerkes erlaubt ist, genehmigt die Firewall die Übertragung der Information an ihren Zielort. Paketfilter-Schutz findet sich in den meisten Firewall-Systemen und wird in der Regel mit der Router-Software implementiert. |
| Anwendungs-Proxy | Prüft, wohin ein Datenpaket übertragen wird und welche Informationsart es enthält. Er erkennt die übertragene Informationsart und übermittelt das Paket an seinen Zielort. Anwendungs-Proxies steuern den Informationsfluß zwischen internen und externen Clients und Servern. Da sich ein Proxy auf Anwendungsebene in der eigentlichen Anwendung befindet und die Kommunikation für denjenigen führt, von dem die Anforderung stammt, bietet er eine größere und besser konfigurierbare Sicherheit als eine Paketfilter-Lösung. Ein HTTP-Proxy ist eine Art von Anwendungs-Proxy, der es Benutzern in einem sicheren Netzwerk gestattet, durch einen Firewall-Server auf das Internet zuzugreifen. Der HTTP-Proxy-Server kommuniziert zwar über das HTTP-Protokoll mit Internet-Benutzern, kann jedoch mit externen Internet-Servern mit seinem eigenen Netzwerkprotokoll kommunizieren, z. B. FTP, Gopher, Remote Procedure Calls (RPC) oder Protokolle, die durch Secure Sockets Layer (SSL) gesichert sind. Wenn ein Benutzer z. B. durch den HTTP-Proxy eine Seite auf einem Gopher-Internet-Server anfordert, ruft der HTTP-Proxy-Server die Seite über Gopher ab und sendet sie dann über HTTP zurück an den Benutzer. |
| Geschalteter oder generischer Proxy | Ein geschalteter Proxy ist einem Anwendungs-Proxy ähnlich, muß jedoch nicht die übertragene Informationsart erkennen. Ein SOCKS-Server kann z. B. als geschalteter Proxy agieren. |

## Szenarien für Serverzugriff

Nachstehende Tabelle beschreibt mehrere Möglichkeiten, den Zugriff auf den Sametime Server zu steuern, und listet die Ergebnisse eines Sametime Clients (Andrew) auf, der versucht, auf eine Datenbank auf dem Server zuzugreifen.

| Szenarienbeschreibung | Ergebnis |
|---|---|
| Schauplatz 1<br>• Auf dem Server ist anonymer Zugriff aktiviert und grundlegende Kennwortauthentifizierung deaktiviert.<br>• Die Datenbank-Zugriffskontrolliste (ACL) gestattet anonymen Benutzern den Zugriff. | Der Server erlaubt Andrew, die Aktionen auszuführen, die anonymen Benutzern in der Datenbank-ACL gewährt werden. |

| | |
|---|---|
| Schauplatz 2<br>• Auf dem Server ist grundlegende Kennwortauthentifizierung und anonymer Zugriff aktiviert.<br>• Die Datenbank-ACL gestattet anonymen Benutzern den Zugriff. | Der Server erlaubt Andrew, die Aktionen auszuführen, die anonymen Benutzern in der Datenbank-ACL gewährt werden. |
| Schauplatz 3<br>• Auf dem Server ist grundlegende Kennwortauthentifizierung und anonymer Zugriff aktiviert.<br>• Die Datenbank-ACL gestattet anonymen Benutzern keinen Zugriff. | Der Server fordert Andrews Namen und Kennwort an. Andrew sendet seinen Namen und sein Kennwort an den Server. Der Server prüft, ob der empfangene Name und das Kennwort mit dem Namen und Kennwort in Andrews Personendokument im öffentlichen Adreßbuch übereinstimmen. Wenn das öffentliche Adreßbuch kein Personendokument für Andrew enthält oder das Kennwort nicht übereinstimmt, wird Andrew der Zugriff auf die Datenbank verweigert. Wenn Andrews Personendokument existiert und das Kennwort übereinstimmt, erlaubt der Server Andrew, die Aktionen auszuführen, die ihm in der Datenbank-ACL gewährt werden. |
| Schauplatz 4<br>• Auf dem Server ist grundlegende Kennwortauthentifizierung aktiviert und anonymer Zugriff deaktiviert.<br>• Die Datenbank-ACL gestattet anonymen Benutzern den Zugriff. | Der Server fordert Andrews Namen und Kennwort an. Andrew sendet seinen Namen und sein Kennwort an den Server. Der Server prüft, ob der empfangene Name und das Kennwort mit dem Namen und dem Kennwort in Andrews Personendokument im öffentlichen Adreßbuch übereinstimmen. Wenn das öffentliche Adreßbuch kein Personendokument für Andrew enthält oder das Kennwort nicht übereinstimmt, wird Andrew der Zugriff auf die Datenbank verweigert. Wenn Andrews Personendokument existiert und das Kennwort übereinstimmt, erlaubt der Server Andrew, die Aktionen auszuführen, die ihm in der Datenbank-ACL gewährt werden. |

# Kapitel 12: Einrichten des Secure Sockets Layer (SSL)

## Secure Sockets Layer- (SSL) Protokoll

Das Secure Sockets Layer- (SSL) Protokoll ist ein RSA-Verschlüsselungssystem mit öffentlichen/privaten Schlüsseln, das private Kommunikation über das Internet oder ein privates Intranet schützt. Web-Browser verwenden das HTTPS-Protokoll, um mit dem Sametime Server über den SSL-Anschluß zu kommunizieren. SSL bietet die höchste Sicherheitsstufe für Internet und Intranet, ist jedoch auch am schwierigsten zu implementieren. Der Sametime Server unterstützt Version 3 des SSL-Protokolls.

SSL verwendet ein eindeutiges Paar mathematischer öffentlicher und privater Schlüssel, um SSL-Transaktionen zu verschlüsseln und zu entschlüsseln. Die öffentliche Schlüsselzulassung steht jedem zur Verfügung und enthält Identifikationsinformation für den Client oder Server, einen öffentlichen Schlüsselwert, den Namen der Zulassungsstelle (CA), die die Zulassung vergeben hat, sowie die digitale Unterschrift der Zulassungsstelle. Der Client oder der Server, der eine SSL-Nachricht empfängt, muß die Nachricht mit Hilfe des öffentlichen/privaten Schlüsselpaars entschlüsseln.

Nachstehende Tabelle erläutert kurz die Sicherheitsvorzüge von SSL.

| Vorteil | Beschreibung |
|---|---|
| Vertraulichkeit | Daten von und an Clients werden verschlüsselt, damit Vertraulichkeit bei Transaktionen gewährleistet ist. |
| Nachrichtenvalidierun g | Eine verschlüsselte Nachrichtenübersicht begleitet Daten, um jegliche Veränderung der Nachricht aufzudecken. |
| Server-Zulassungs-authentifizierung | Die Server-Zulassung begleitet Nachrichten, um dem Client zu garantieren, daß die Server-Identität authentisch ist. |
| Client-Zulassungs-authentifizierung | Die Client-Zulassung begleitet Nachrichten, um dem Server zu garantieren, daß die Client-Identität authentisch ist. Client-Zulassungsauthentifizierung ist optional. Sie können anonymen Zugriff auf den Server gestatten oder von Benutzern grundlegende Kennwortauthentifizierung verlangen. |

Zugriff auf den Inhalt des Servers wird durch die Zugriffskontrolliste (ACL) einer Datenbank gesteuert. Die Datenbank-ACL definiert Rollen für Benutzer und deren Möglichkeiten, den Inhalt der Datenbank zu nutzen. Sie können die Datenbank-Zugriffskontrolliste (ACL) einrichten, um die erlaubte Zugriffsebene auf die Datenbank für anonyme Benutzer festzulegen.

Die Einstellung "Max. Internet-Namen- & Kennwortzugriff" im Fenster "Erweitert" jeder Datenbank-ACL ist ohne Wirkung, wenn Benutzer Verbindungen über SSL aufbauen.

## SSL-Zulassungen

SSL-Sicherheit beruht auf Client- und Server-Zulassungen. Der Sametime Server verwendet das gängige SSL-Zulassungsformat, das durch die International Telecommunication Union (ITU) Recommendation X.509, *The Directory - Authentication Framework* definiert ist. Zulassungen lassen sich zwischen dem Sametime Server und anderen Anwendungen, die dieses Format einhalten, auf einfache Weise austauschen.

Zulassungen werden von einer Zulassungsstelle (CA) ausgestellt. Die CA ist eine vertrauenswürdige Drittfirma, die für die Identität des Servers und Clients garantiert. Für Internet-Transaktionen muß die CA eine weithin bekannte und vertrauenswürdige Einrichtung sein, wie z. B. VeriSign. Für Ihr Intranet können Sie auch eine interne Zulassung verwenden, z. B. die Anwendung Sametime Zulassungsstelle.

Client-Zulassungen werden durch den Browser des Clients verwaltet, Server-Zulassungen werden in der Schlüsselringdatei auf der Festplatte des Servers gespeichert. Eine Schlüsselringdatei ist eine kennwortgeschützte binäre Datei, die eine oder mehrere Zulassungen sowie die anerkannte Root-Zulassung von CAs enthält, die der Server erkennt.

Jede Zulassung enthält die folgende Information:

- den öffentlichen Schlüssel des Eigentümers,
- den eindeutigen Namen des Eigentümers,

- das Ablaufdatum der Zulassung,
- den Namen der CA, die die Zulassung ausgestellt hat,
- die digitale Unterschrift der CA.

Die digitale Unterschrift der CA wird auf die Client- und Server-Zulassungen gestempelt und gewährleistet, daß der entsprechende Server oder Client anerkannt ist. Der Browser des Clients identifiziert den Server, indem er die digitale Unterschrift auf der Server-Zulassung mit der öffentlichen Zulassung des Servers vergleicht. Wenn die Authentifizierung von Client-Zulassungen aktiviert ist, identifiziert der Sametime Server einen Client, indem er die digitale Unterschrift auf der Client-Zulassung mit der anerkannten Root-Zulassung der CA in der Schlüsselringdatei vergleicht. Wenn Server und Client einander identifizieren können, kann eine sichere SSL-Sitzung aufgebaut werden. Andernfalls wird die Sitzung nicht eingerichtet.

Der eindeutige Name des Eigentümers verfügt über mehrere erforderliche und optionale Komponenten. Je mehr Komponenten Sie angeben, um so geringer ist die Möglichkeit, auf einen identischen Namen im Internet zu treffen.

Verwandte Themen anzeigen
Zulassungsstellen
Die Anwendung "Zulassungsstelle"
Eindeutige Namen
Beispiel einer SSL-Validierung und Authentifizierung

## Eindeutige Namen

Nachstehende Tabelle beschreibt kurz die Komponenten der eindeutigen Namen.

| **Komponente** | **Beschreibung** |
|---|---|
| Allgemeiner Name (erforderlich) | Beschreibender Name, der den Benutzer identifiziert. Der allgemeine Name eines Servers ist der vollständige TCP/IP-Hostname, wie z. B. www.lotus.com. Da einige Browser den allgemeinen Namen mit dem Hostnamen vergleichen, bevor sie eine Verbindung aufbauen, sollten Sie in der Server-Zulassung für den allgemeinen Namen den Hostnamen angeben, der im Feld "Host" des Serverdokuments erscheint. |
| Abteilung (optional) | Abteilung, in der der Eigentümer arbeitet. |
| Unternehmen (erforderlich) | Name des Unternehmens, in dem der Eigentümer arbeitet. In der Regel ist dies der Firmenname, z. B. Acme. |
| Ort (optional) | Stadt oder Ort, in der der Eigentümer wohnt. |
| Bundesland oder Region (erforderlich) | Aus mindestens drei Zeichen bestehender Name, der das Bundesland bzw. die Region angibt, in der der Eigentümer wohnt, z. B. Bayern. (Geben Sie für US-Staaten den vollständigen Namen ein, nicht die Abkürzung.) |
| Land (erforderlich) | Aus zwei Zeichen bestehendes Kürzel für das Land, in dem der Eigentümer wohnt, verwenden Sie z. B. US für Vereinigte Staaten und CA für Kanada. |

Verwandte Themen anzeigen
Zulassungsstellen
SSL-Zulassungen

## Zulassungsstellen

Zulassungsstellen (CAs) sind verantwortlich für das Ausstellen von Zulassungen, die Clients oder Server bei Verwendung von SSL identifizieren. Die CA stellt ein öffentlich/privates Schlüsselpaar aus, das den Client eindeutig beim Server identifiziert. Eine Zulassungsstelle kann extern und kommerziell arbeiten, wie z. B. VeriSign, oder intern in Ihrem Unternehmen eingerichtet werden. In der Regel richten Sie Clients und Server für das Internet mit Hilfe einer externen Zulassungsstelle ein, die sowohl Server- als auch Client-Zulassungen ausstellen kann. Für Ihr Intranet können Sie eine interne Zulassung verwenden, z. B. die Anwendung Sametime Zulassungsstelle.

Eine anerkannte Zulassungsstelle unterzeichnet die öffentlich/privaten Schlüsselpaare und überträgt sie sicher an den Client oder Server. Sie können allen Servern und Clients vertrauen, die eine gültige digitale Unterschrift von einer Zulassungsstelle aufweisen, für die die Schlüsselringdatei des Servers eine anerkannte Root-Zulassung enthält.

Verwandte Themen anzeigen
Die Anwendung "Zulassungsstelle"
Anerkannte SSL-Roots

## Internet-Server-Zulassungen

Wenn Benutzer außerhalb Ihres Unternehmens über SSL auf Ihren Server zugreifen sollen, müssen Sie eine Zulassung von einer externen Zulassungsstelle (CA) beziehen, z. B. von VeriSign. Die externe CA dient als anerkannte Drittfirma, damit unbekannte Server und Clients sicher miteinander kommunizieren können.

Wenn Sie eine Server-Zulassung erhalten möchten, müssen Sie zunächst eine Schlüsselringdatei anlegen und dann eine Zulassungsanforderung im Standardformat Public Key Cryptography Standards (PKCS) an die CA richten. PKCS ist ein Format, das viele CAs erkennen, einschließlich des Sametime Servers. Stellen Sie sicher, daß die CA dieses Format und nicht etwa ein anderes wie Privacy-Enhanced Mail (PEM) verwendet, bevor Sie eine Anforderung senden. Wenn Sie eine Zulassung von einer CA anfordern, geben Sie die Schlüsselringdatei an, die die Zulassung speichert, sowie den anerkannten Namen für Ihren Server.

Wenn die CA die Anforderung empfängt, entscheidet sie, ob die Anforderung genehmigt wird. Wenn die Anforderung genehmigt ist, fordert Sie die CA auf, Ihre Anforderung abzuholen. Sie können dann die Zulassung in Ihre Schlüsselringdatei mischen. Auf welche Weise die CA die Benachrichtigung sendet, hängt von der CA ab. In den meisten Fällen sendet die CA entweder die unterzeichnete ID als E-Mail-Anlage oder eine URL, die angibt, wo Sie die ID abholen können.

Verwandte Themen anzeigen
Eindeutige Namen
Erstellen eines Schlüsselrings und einer Server-Zulassungsanforderung

## Intranet-Server-Zulassungen

Sie müssen eine Server-Zulassung von einer internen Zulassungsstelle (CA) anfordern, um mit anderen Clients und Servern in Ihrem Unternehmen zu kommunizieren. Alle Server und Clients, die von der CA als anerkanntes Root markiert sind, können mit dem Server kommunizieren.

Wenn Sie ein Server-Zulassung erhalten möchten, müssen Sie zunächst eine Schlüsselringdatei anlegen und dann eine Anforderung einer Zulassung im Standardformat Public-Key Cryptography Standards (PKCS) an die interne CA richten. Wenn Sie eine Zulassung von einer CA anfordern, geben Sie die Schlüsselringdatei an, die die Zulassung speichert, sowie den eindeutigen Namen für Ihren Server.

Wenn die CA die Anforderung empfängt, entscheidet sie, ob die Anforderung genehmigt wird. Wenn die Anforderung genehmigt ist, fordert Sie die CA auf, Ihre Anforderung über Ihren Browser in der Anwendung "Zulassungsstelle" abzuholen. Die CA liefert entweder eine URL, die den Speicherort der ID angibt, oder eine Abhol-ID, die Sie in die Anwendung "Zulassungsstelle" eingeben. Sie können dann die Zulassung in Ihre Schlüsselringdatei mischen.

Verwandte Themen anzeigen
Eindeutige Namen
Erstellen eines Schlüsselrings und einer Server-Zulassungsanforderung

## Beispiel einer SSL-Validierung und Authentifizierung

Das folgende Beispiel veranschaulicht, wie ein Benutzer (Hugo) mit Hilfe des SSL-Protokolls eine Verbindung zu einem Server (ServerA) aufbaut.

1. Hugo sendet eine Anforderung an ServerA, in der er Informationen über die SSL-Verbindung angibt, z. B. unterstützte Verschlüsselungsalgorithmen und das Ablaufdatum der Zulassung.
2. ServerA sendet Hugo seine Zulassung, die den öffentlichen Schlüssel von ServerA enthält. Hugo prüft die digitale Unterschrift der Zulassungsstelle auf der Zulassung, um die Identität von ServerA zu verifizieren. Wenn die digitale Unterschrift in der Zulassung von ServerA unbefugt verändert wurde, kann ServerA nicht verifiziert werden.
3. Hugo verwendet einen Algorithmus, um ein geheimes Verschlüsselungspaar zu erzeugen, verschlüsselt den geheimen Schlüssel mit Hilfe des öffentlichen Schlüssels, der in der Zulassung von ServerA gespeichert ist, und sendet ihn an ServerA. Dieser geheime Schlüssel ändert sich für jede Sitzung, wodurch er schwierig aufzudecken ist.
4. ServerA dekodiert den geheimen Schlüssel mit Hilfe des privaten Schlüssels von ServerA und verwendet den geheimen Schlüssel zur Verschlüsselung der Daten, die anschließend zwischen Hugo und ServerA übertragen werden.
5. Wenn "Zulassung" auf Benutzerseite aktiviert ist, fordert ServerA Hugos Zulassung an.
6. Hugo sendet seine Zulassung an ServerA, der wiederum die digitale Unterschrift auf Hugos Zulassung überprüft, um die Identität von Hugo zu verifizieren. Wenn die digitale Unterschrift in Hugos Zulassung unbefugt verändert wurde, kann Hugo nicht verifiziert werden.
7. Wenn Hugo nicht verifiziert wird, verwendet der Server dieselbe Methode, um Namen und Kennwort und anonymen Zugriff zu verifizieren.

## Die Anwendung "Zulassungsstelle"

Die Anwendung "Zulassungsstelle" (CERTCA.NSF) ermöglicht Ihnen, eine interne Zulassungsstelle (CA) in Ihrem Unternehmen aufzubauen. Eine interne CA ist verantwortlich für die Verarbeitung von Zulassungsanforderungen von Sametime Server Administratoren in Ihrem Unternehmen und für die Aufnahme von Client-Zulassungen in das Sametime Adreßbuch. Durch Einrichten einer internen CA vereinfachen Sie das Verfahren für das Anlegen und Verwalten von Zulassungen, wenn Benutzer nicht mit externen Servern kommunizieren müssen oder wenn externe Benutzer nicht auf Ihre Server zugreifen müssen. Außerdem vermeiden Sie damit unnötige Gebühren, die externe CAs für das Ausstellen und Bestätigen von Zulassungen verlangen.

Wenn Sie die Anwendung "Zulassungsstelle" ändern möchten, legen Sie die Datenbank CERTCA.NSF mit Hilfe der Schablone "Zulassungsstelle" (CCA461.NTF) an und aktivieren Sie Datenbank- und Serversicherheit.

Sie können auf die Anwendung "Zulassungsstelle" mit Hilfe eines Notes Clients auf dem Server zugreifen. Sie können auch von einer fernen Workstation auf die Anwendung zugreifen, jedoch müssen Sie zuvor die Schlüsselringdatei auf die Workstation kopieren.

Mit Hilfe der Anwendung "Zulassungsstelle" können Sie die CA-Zulassung und die Schlüsselringdatei erstellen, Server- und Client-Zulassungen unterzeichnen und Client-Zulassungen in das Sametime Adreßbuch aufnehmen. Server-Administratoren und Clients senden ihre Zulassungsanforderungen an diese Datenbank und verwenden einen Browser, um genehmigte Zulassungen und anerkannte Root-Zulassungen abzuholen.

Verwandte Themen anzeigen
Einrichten der Anwendung "Zulassungsstelle"
Anerkannte SSL-Roots
Erstellen eines CA-Schlüsselrings und einer CA-Zulassung

## Anerkannte SSL-Roots

Der Sametime Server enthält einen Satz von anerkannten Standard-Root-Zulassungen von mehreren bekannten externen Zulassungsstellen (CAs). Anerkannte Root-Zulassungen gestatten Clients und Servern, mit jedem Client oder Server zu kommunizieren, der eine Zulassung von dieser CA besitzt. Diese anerkannten Standard-Root-Zulassungen werden in die Client- oder Server-Schlüsselringdatei gemischt, um das Einrichten von Client-Authentifizierung für einen Client zu vereinfachen, der eine Zulassung von einer der Standard-CAs erhalten hat.

Der Sametime Server umfaßt die folgenden anerkannten Root-Zulassungen, wenn Sie eine Server-Schlüsselringdatei anlegen:

**VeriSign Class 4 Public Primary Certification Authority**

Unternehmen: VeriSign, Inc.

Abteilung: Class 4 Public Primary Certification Authority

Land: US

**VeriSign Class 3 Public Primary Certification Authority**

Unternehmen: VeriSign, Inc.

Abteilung: Class 3 Public Primary Certification Authority

Land: US

**VeriSign Class 2 Public Primary Certification Authority**

Unternehmen: VeriSign, Inc.

Abteilung: Class 2 Public Primary Certification Authority

Land: US

**VeriSign Class 1 Public Primary Certification Authority**

Unternehmen: VeriSign, Inc.

Abteilung: Class 1 Public Primary Certification Authority

Land: US

**RSA Secure Server Certificate Authority**

Unternehmen: RSA Data Security, Inc.

Abteilung: Secure Server Certification Authority

Land: US

**Netscape Test Certificate Authority**

Unternehmen: Netscape Communications Corp.

Abteilung: Test CA

Land: US

**RSA Low Assurance Certificate Authority**

Unternehmen: RSA Data Security, Inc.

Abteilung: Low Assurance Certification Authority

Land: US

**VeriSign Persona Certificate Authority**

Unternehmen: RSA Data Security, Inc.

Abteilung: Persona Certificate

Land: US

Verwandte Themen anzeigen
Die Anwendung "Zulassungsstelle"

## Die Anwendung "Server-Zulassungsadministration"

Die Anwendung "Server-Zulassungsadministration" (CERTSRV.NSF) gestattet Ihnen, Server-Zulassungen von einer internen oder externen Zulassungsstelle (CA) anzufordern und Ihre Server-Zulassungen in einer Schlüsselringdatei zu verwalten. Um diese Anwendung zu verwenden, müssen Sie die Datenbank CERTSRV.NSF anlegen und einrichten. Für den Zugriff auf die Anwendung "Server-Zulassungsadministration" müssen Sie eine Notes Workstation oder einen Notes Client auf dem Server verwenden.

Zu Testzwecken können Sie in der Anwendung "Server-Zulassungsadministration" auch die Server-Zulassung und die Schlüsselringdatei anlegen, die Zulassung einer CA als vertrauenswürdiges Root hinzufügen und eine selbst ausgestellte Zulassung erzeugen.

## Einrichten von SSL auf einem Server

Für den Einsatz von SSL auf dem Sametime Server für sichere Transaktionen, Validieren von Nachrichten, Authentifizieren von Server-Identitäten und optionale Authentifizierung von Client-Identitäten müssen die folgenden Voraussetzungen erfüllt sein:

- Die Server müssen über Zulassungen von einer internen oder externen Zulassungsstelle (CA) verfügen.
- Die Clients müssen die CA-Zulassung des Servers als anerkanntes Root markiert haben.
- (Optional) Für grundlegende Kennwortauthentifizierung muß jeder Client über ein Personendokument verfügen, das ein Internet-Kennwort enthält.
- (Optional) Für Zulassungsauthentifizierung muß jeder Client über eine Zulassung von einer internen oder externen CA oder ein Personendokument verfügen, das die SSL-Zulassung mit dem öffentlichen Schlüssel enthält. Der Server muß die CA-Zulassung des Clients als anerkanntes Root markiert haben.

Sie richten SSL auf einem Server ein, indem Sie die folgenden Aktionen ausführen:

1. Richten Sie die Anwendung "Zulassungsstelle" ein.
2. Richten Sie die Anwendung "Server-Zulassungsadministration" ein.
3. Mischen Sie die Zulassung der CA als anerkanntes Root in die Schlüsselringdatei.
4. Legen Sie einen Schlüsselring an, und fordern Sie eine Server-Zulassung von einer CA an.
5. Mischen Sie die unterzeichnete Zulassung in die Server-Schlüsselringdatei ein.
6. Konfigurieren Sie das Serverdokument so, daß SSL für Server-Tasks aktiviert ist.
7. Richten Sie optional den Server oder einzelne Datenbanken so ein, daß sie SSL-Verbindungen verlangen.
8. Fügen Sie Datenbank-Zugriffskontrollisten Client-Namen hinzu, wenn Sie Client-Zulassung- oder grundlegende Kennwortauthentifizierung auf dem Server einrichten.

**Hinweis** Richten Sie SSL nicht auf einem Web-Server ein, der für mehrere Sites als Host dient. Der Sametime Server unterstützt SSL nur auf Servern, die Host für eine einzige Site sind.

Verwandte Themen anzeigen
Einrichten der Anwendung "Zulassungsstelle"
Die Anwendung "Server-Zulassungsadministration"
Mischen einer Zulassung von einer Internet-Zulassungsstelle als anerkanntes Root
Mischen einer Zulassung von einer Intranet-Zulassungsstelle als anerkanntes Root
Erstellen eines Schlüsselrings und einer Server-Zulassungsanforderung
Mischen einer Internet-Server-Zulassung
Mischen einer Intranet-Server-Zulassung
Konfigurieren des Serverdokuments für SSL
Einrichten von Servern für automatische SSL-Verbindung von Clients

## Einrichten der Anwendung "Zulassungsstelle"

Mit Hilfe der Anwendung "Zulassungsstelle" können Sie eine interne Zulassungsstelle (CA) in Ihrem Unternehmen einrichten. Gehen Sie wie folgt vor, um die Anwendung "Zulassungsstelle" zu erzeugen und einzurichten:

1. Legen Sie auf dem Server mit Hilfe des Notes Clients und der Schablone CCA461.NTF die Datenbank CERTCA.NSF an.

   **Hinweis** Sie müssen beim Anlegen der Datenbank die Option "Weitere Schablonen anzeigen" aktivieren, um die Schablone CCA461.NTF zu sehen.

2. Führen Sie in der Zugriffskontrolliste (ACL) der Datenbank "Zulassungsstelle" folgende Aktionen aus:
   - Fügen Sie die Namen der Personen hinzu, die Zulassungen verwalten sollen, und weisen Sie ihnen Editorenzugriff mit Löscherlaubnis sowie die Rolle CAPrivilegedUser zu.
   - Stellen Sie den Standardzugriff auf "Autor" mit Erstellungserlaubnis ein.
3. (Optional) Um diese Datenbank auszublenden, wenn Benutzer Datenbanken über "Datei - Datenbank - Öffnen" öffnen oder wenn Browser-Benutzer eine Datenbankliste anzeigen, deaktivieren Sie "Im Dialogfeld "Datenbank öffnen" im Feld "Datenbank".
4. Wenn Ihre Clients Netscape Navigator verwenden, öffnen Sie das Eigenschaftenfeld der Anwendung "Zulassungsstelle". Aktivieren Sie "Web-Zugriff: SSL-Verbindung anfordern" in der Registerkarte "Allgemein", um bei Verbindungen von Browsern zu dieser Datenbank die Verwendung von SSL zu erzwingen.

**Hinweis** Wenn Ihre Clients Microsoft Internet Explorer verwenden, erzwingen Sie nicht den Datenbankzugriff mit SSL. Internet Explorer gestattet Clients nicht, in ihren Browser eine Site-Zulassung für einen Server zu übernehmen, für den sie über keine anerkannte Root-Zulassung verfügen. Clients müssen über TCP/IP auf die Datenbank zugreifen, um die Zulassung als anerkanntes Root zu mischen.

## Einrichten der Anwendung "Server-Zulassungsadministration"

Mit Hilfe der Anwendung "Server-Zulassungsadministration" können Sie Server-Zulassungen von einer internen oder externen Zulassungsstelle (CA) anfordern und Ihre Server-Zulassungen in einer Schlüsselringdatei verwalten. Gehen Sie wie folgt vor, um die Anwendung "Server-Zulassungsadministration" zu erstellen und einzurichten:

1. Legen Sie auf dem Server mit Hilfe des Notes Clients und der Schablone CCA461.NTF die Datenbank CERTCA.NSF an.

   **Hinweis** Sie müssen beim Anlegen der Datenbank die Option "Weitere Schablonen anzeigen" aktivieren, um die Schablone CCA461.NTF zu sehen.

2. Stellen Sie in der Zugriffskontrolliste (ACL) der Datenbank "Server-Zulassungsadministration" den Standardzugriff auf "Kein Zugriff" ein, damit andere die Datenbank nicht verwenden können.
3. (Optional) Um diese Datenbank auszublenden, wenn Benutzer Datenbanken über "Datei - Datenbank - Öffnen" öffnen oder wenn Browser-Benutzer eine Datenbankliste anzeigen, deaktivieren Sie "Im Dialogfeld 'Datenbank öffnen'" im Feld "Datenbank".

**Hinweis** Sie müssen Server-Administratoren in der ACL keinen Zugriff zuweisen, da sie lokal auf die Anwendung "Server-Zulassungsadministration" zugreifen.

### Mischen einer Zulassung von einer Internet-Zulassungsstelle als anerkanntes Root

Bevor Sie eine Zulassung installieren, die von einer Zulassungsstelle (CA) unterzeichnet ist, wird dringend empfohlen, daß Sie die Zulassung der CA in Ihre Schlüsselringdatei als anerkanntes Root mischen.

1. Überprüfen Sie die anerkannten Roots in der Schlüsselringdatei, um festzustellen, ob die Zulassung der CA bereits existiert. Falls sie existiert, müssen Sie die folgenden Schritte nicht ausführen.
2. Beziehen Sie die anerkannte Root-Zulassung von der Web-Site der CA. In den meisten Fällen ist die Zulassung eine Anlage zu einer Datei oder kann in die Zwischenablage kopiert werden.
3. Klicken Sie in Notes im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Server-Zulassungsadministrationsdatenbank öffnen" (CERTSRV.NSF) auf dem lokalen Rechner.
4. Klicken Sie auf "Installieren Sie eine anerkannte Root-Zulassung im Schlüsselring".
5. Geben Sie den Namen der Schlüsseldatei für den Schlüsselring ein, die diese Zulassung speichern soll. Sie haben den Namen der Schlüsselringdatei eingegeben, als Sie die Anforderung für die Server-Zulassung erstellt haben.
6. Geben Sie einen Namen für diese Zulassung ein, unter dem sie in der Schlüsselringdatei angezeigt werden soll.
7. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie in Schritt 2 den Inhalt der Zulassung der CA in die Zwischenablage kopiert haben, aktivieren Sie "Zwischenablage" im Feld "Quelle der Zulassung". Fügen Sie den Inhalt der Zwischenablage in das nächste Feld ein.
   - Wenn Sie in Schritt 2 eine Datei erhalten haben, die die Zulassung der CA enthält, speichern Sie die Datei auf Ihrer Festplatte und aktivieren Sie "Datei" im Feld "Quelle der Zulassung". Geben Sie den Dateinamen in das Feld "Dateiname" ein.
8. Klicken Sie auf "Anerkanntes Root in Schlüsselring mischen".
9. Geben Sie das Kennwort für die Schlüsselringdatei ein, und klicken Sie auf OK.

Verwandte Themen anzeigen
Anerkannte SSL-Roots
Anzeigen Ihrer Server-Zulassungen

### Mischen einer Zulassung von einer Intranet-Zulassungsstelle als anerkanntes Root

1. Blättern Sie zur Datenbank "Zulassungsstelle" in der Web-Site der internen Zulassungsstelle (CA).
2. Wenn Sie Microsoft Internet Explorer verwenden, bauen Sie eine TCP/IP-Verbindung zum Server auf. Internet Explorer erlaubt keine Übernahme von Web-Site-Zulassungen in Ihren Browser.
3. Wenn Sie Netscape verwenden, sollten Sie eine Verbindung zur Anwendung "Zulassungsstelle" über SSL aufbauen. Akzeptieren Sie die Übernahme der Zulassung in Ihren Browser, indem Sie die Anleitungen der Browser-Software befolgen.
4. Klicken Sie im linken Fensterbereich auf "Accept This Authority in Your Server".
5. Kopieren Sie die Zulassung in die Zwischenablage, einschließlich der Zeilen "Beginn Zulassung" und "Ende Zulassung".
6. Klicken Sie in Notes im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Server-Zulassungsadministration öffnen" (CERTSRV.NSF) auf dem lokalen Rechner.
7. Klicken Sie auf "Installieren Sie eine anerkannte Root-Zulassung im Schlüsselring".
8. Geben Sie den Namen der Schlüsseldatei für den Schlüsselring ein, die diese Zulassung speichern soll. Sie haben den Namen der Schlüsselringdatei eingegeben, als Sie die Anforderung für die Server-Zulassung erstellt haben.

9. Geben Sie einen Namen für diese Zulassung ein, unter dem die Zulassung in der Schlüsselringdatei angezeigt werden soll. Wenn dieses Feld leer ist, verwendet der Sametime Server den eindeutigen Namen zur Identifikation der Zulassung.
10. Aktivieren Sie "Zwischenablage" im Feld "Quelle der Zulassung". Fügen Sie den Inhalt der Zwischenablage in das nächste Feld ein.
11. Klicken Sie auf "Anerkanntes Root in Schlüsselring mischen".
12. Geben Sie das Kennwort für die Schlüsselringdatei ein, und klicken Sie auf "OK".

Verwandte Themen anzeigen
  Die Anwendung "Zulassungsstelle"
  Anerkannte SSL-Roots

## Erstellen eines Schlüsselrings und einer Server-Zulassungsanforderung

Folgen Sie nachstehenden Schritten, um eine Schlüsselringdatei und eine Anforderung einer Server-Zulassung zu erstellen, die an eine interne Zulassungsstelle (CA) oder eine anerkannte kommerzielle Zulassungsstelle wie VeriSign gesendet werden kann.

1. Klicken Sie im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Server-Zulassungsadministration öffnen" (CERTSRV.NSF) auf dem lokalen Rechner.
2. Klicken Sie auf "Erstellen Sie einen Schlüsselring".
3. Geben Sie einen Namen für die Schlüsselringdatei in das Feld "Name der Schlüsselringdatei" ein.
4. Geben Sie ein Kennwort für die Server-Schlüsselringdatei in das Feld "Schlüsselringkennwort" ein.

   **Hinweis** Das Kennwort ist eine alphanumerische Zeichenfolge, die den Schlüsselring vor unbefugtem Zugriff schützt. Groß- und Kleinschreibung wird dabei unterschieden. Sie sollten mindestens zwölf alphanumerische Zeichen für das Kennwort eingeben.
5. Wählen Sie eine Schlüsselgröße. Der Sametime Server verwendet diese Schlüsselgröße beim Erzeugen öffentlicher und privater Schlüsselpaare. Je größer der Schlüssel, um so stärker ist die Verschlüsselung. Wenn Sie eine internationale Version des Sametime Servers verwenden, steht nur eine Schlüsselgröße von 512 Bit zur Verfügung.
6. Geben Sie die Komponenten des unterscheidbaren Namens Ihres Servers ein.
7. Klicken Sie auf "Schlüsselring erstellen".
8. Wenn Sie die Information über die Schlüsselringdatei und den eindeutigen Servernamen gelesen haben, klicken Sie auf OK.
9. Klicken Sie auf "Erstellen Sie eine Zulassungsanforderung".
10. Führen Sie eine der folgenden Aktionen aus:
    - Klicken Sie auf "Als E-Mail an CA senden" und geben Sie die E-Mail-Adresse der CA sowie Ihre E-Mail-Adresse, Telefonnummer und Ihren Standort ein.
    - (Empfohlen) Klicken Sie auf "In Maske auf CA Site einfügen".

    **Hinweis** Verwenden Sie "In Maske auf CA Site einfügen", wenn Sie eine Anforderung an eine interne CA oder an VeriSign senden. VeriSign verwendet das PKCS-Format nicht für Anforderungen, die per E-Mail eingehen.
11. Wenn Sie Information über diese Anforderung in der Anwendung Server-Zulassungsadministration protokollieren wollen, aktivieren Sie "Ja" im Feld "Zulassungsanforderung protokollieren". Aktivieren Sie andernfalls "Nein".
12. Klicken Sie auf "Zulassungsanforderung erstellen".
13. Geben Sie das Kennwort für die Schlüsselringdatei ein, das Sie in Schritt 4 angegeben haben.
14. Wenn Sie in Schritt 10 "In Maske auf CA Site einfügen" aktiviert haben, führen Sie folgende Aktionen aus:
    - Markieren Sie den Text im Dialogfenster.
    - Drücken Sie STRG+C, um den ausgewählten Text in die Zwischenablage zu kopieren.
    - Klicken Sie auf OK.

**Hinweis** Sie müssen sämtlichen Text im zweiten Dialogfenster auswählen, einschließlich der Zeilen "Beginn Zulassung" und "Ende Zulassung".

15. Verwenden Sie für eine externe CA einen Browser, um die Site der CA zu besuchen, und folgen Sie den Anleitungen für das Senden einer neuen Zulassungsanforderung.
16. Führen Sie für eine interne CA folgende Aktionen aus:
    - Blättern Sie zur Datenbank "Zulassungsstelle" in der Web-Site der CA.
    - Wenn Sie Microsoft Internet Explorer verwenden, bauen Sie eine TCP/IP-Verbindung zum Server auf. Internet Explorer erlaubt keine Übernahme von Web-Site-Zulassungen in Ihren Browser.
    - Wenn Sie Netscape verwenden, sollten Sie eine Verbindung zur Anwendung "Zulassungsstelle" über SSL aufbauen. Akzeptieren Sie die Übernahme des Zertifikats in Ihren Browser, indem Sie die Anleitungen der Browser-Software befolgen.
    - Klicken Sie auf "Server-Zulassung anfordern".
    - Geben Sie Ihren Namen, Ihre E-Mail-Adresse, Telefonnummer und etwaige Kommentare für die CA ein.
    - Fügen Sie Ihre Zulassung in das Dialogfenster ein, und klicken Sie auf "Submit Certificate Request".

Verwandte Themen anzeigen
SSL-Zulassungen
Internet-Server-Zulassungen
Intranet-Server-Zulassungen
Anzeigen von Anforderungen für Server-Zulassungen

## Mischen einer Internet-Server-Zulassung

Nachdem Sie die Zulassung der Zulassungsstelle (CA) als anerkanntes Root gemischt haben und die CA Ihre Server-Zulassungsanforderung genehmigt hat, mischen Sie die unterzeichnete Zulassung in die Schlüsselringdatei.

1. Holen Sie die Zulassung gemäß den Anleitungen der CA ab. In den meisten Fällen sendet eine CA die Zulassung als Dateianlage oder gibt Ihnen eine URL, von der Sie die Zulassung in die Zwischenablage kopieren und einfügen können.
2. Klicken Sie in Notes im Administrationsfenster auf "Systemdatenbanken" und wählen Sie "Server-Zulassungsadministration öffnen" (CERTSRV.NSF) auf dem lokalen Rechner.
3. Klicken Sie auf "Installieren Sie eine anerkannte Root-Zulassung im Schlüsselring".
4. Geben Sie den Namen der Schlüsseldatei für den Schlüsselring ein, die diese Zulassung speichern soll. Sie haben diese Schlüsselringdatei angelegt, als Sie die Anforderung für die Server-Zulassung erstellt haben.
5. Führen Sie eine der folgenden Aktionen aus:
    - Wenn Sie in Schritt 1 den Inhalt der Zulassung der CA in die Zwischenablage kopiert haben, aktivieren Sie "Zwischenablage" im Feld "Quelle der Zulassung". Fügen Sie den Inhalt der Zwischenablage in das nächste Feld ein.
    - Wenn Sie in Schritt 1 eine Datei erhalten haben, die die Zulassung der CA enthält, speichern Sie die Datei auf Ihrer Festplatte und aktivieren Sie "Datei" im Feld "Quelle der Zulassung". Geben Sie den Dateinamen in das Feld "Dateiname" ein.
6. Klicken Sie auf "Anerkannte Root-Zulassung in Schlüsselring mischen".
7. Geben Sie das Kennwort für die Server-Schlüsselringdatei ein, und klicken Sie auf OK, um das Mischen zu bestätigen.

## Mischen einer Intranet-Server-Zulassung

Wenn die Zulassungsstelle (CA) Ihre Anforderung genehmigt, mischen Sie die unterzeichnete Zulassung in die Schlüsselringdatei.

1. Wenn Sie von der CA per E-Mail eine URL erhalten haben, blättern Sie zu dieser URL, um die Zulassung aus der Datenbank-Zulassungsstelle abzuholen.
2. Falls erforderlich erfragen Sie die Pickup-ID bei der CA, und führen Sie folgende Aktionen aus:
   - Öffnen Sie die Datenbank "Zulassungsstelle" mit einem Browser.
   - Klicken Sie auf "Pickup-Server-Zulassung".
   - Geben Sie die Pickup-ID ein, und klicken Sie auf "Pick Up Signed Certificate".
3. Kopieren Sie die Zulassung einschließlich der Zeilen "Beginn Zulassung" und "Ende Zulassung" in die Zwischenablage.
4. Klicken Sie in Notes im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Server-Zulassungsadministration öffnen" (CERTSRV.NSF) auf dem lokalen Rechner.
5. Klicken Sie auf "Installieren Sie eine Zulassung im Schlüsselring".
6. Geben Sie den Namen der Schlüsseldatei für den Schlüsselring ein, die diese Zulassung speichern soll. Sie haben diese Schlüsselringdatei angelegt, als Sie die Anforderung für die Server-Zulassung erstellt haben.
7. Aktivieren Sie "Zwischenablage" im Feld "Quelle der Zulassung". Fügen Sie den Inhalt der Zwischenablage in das nächste Feld ein.
8. Klicken Sie auf "Zulassung in Schlüsseldatei mischen".
9. Geben Sie das Kennwort für die Schlüsselringdatei ein, und klicken Sie auf OK, um das Mischen zu bestätigen.

**Hinweis** Sie erhalten eine Warnmeldung, wenn Sie versuchen, die Server-Zulassung zu mischen, ohne sie zuvor als anerkanntes Root gemischt zu haben. Sie können zwar nach dieser Warnung fortfahren, die Zulassung zu mischen, jedoch kann die Unterschrift auf der Server-Zulassung nicht mit der Zulassung der CA verglichen werden. Dies ist nur möglich, wenn Sie zuerst die Zulassung der CA als anerkanntes Root mischen.

## Konfigurieren des Serverdokuments für SSL

1. Klicken Sie im Sametime Administrationswerkzeug auf "Server" und anschließend auf "Server".
2. Wählen Sie das Serverdokument für den Server aus.
3. Wählen Sie den Abschnitt "Konfiguration für Internet-Anschlüsse und Sicherheit".

4. Aktivieren Sie im Feld "SSL-Protokollversion" eine der folgenden Optionen:

   **Hinweis** Diese Einstellung gilt nur für LDAP-Verbindungen.

   - Nur V2.0 -- Gestattet nur SSL 2.0-Verbindungen.
   - V3.0 Handshake -- Versucht eine SSL 3.0-Verbindung. Wenn diese Verbindung fehlschlägt und der Anforderer SSL 2.0 erkennt, wird eine SSL 2.0-Verbindung versucht.
   - Nur V3.0 -- Gestattet nur SSL 3.0-Verbindungen.
   - V3.0 und V2.0 Handshake -- Versucht eine SSL 3.0-Verbindung, beginnt jedoch mit einem SSL 2.0-Handshake, der relevante Fehlermeldungen anzeigt. Baut eine SSL 3.0-Verbindung auf, falls möglich.
   - Vereinbart -- (Standard) Versucht eine SSL 3.0-Verbindung. Wenn diese Verbindung fehlschlägt, wird eine SSL 2.0-Verbindung versucht. Verwenden Sie diese Einstellung, es sei denn, es treten Verbindungsprobleme aufgrund inkompatibler Protokollversionen auf.
5. Geben Sie in das Feld "SSL-Schlüsselringdatei" den Namen der Schlüsselringdatei ein, die der Server verwendet.
6. Sie stellen ein bestimmtes Protokoll für SSL ein, indem Sie folgende Optionen in der Spalte für das entsprechende Protokoll ändern:

- Wählen Sie "Aktiviert" im Feld "SSL-Anschlußstatus".
- Ändern Sie falls erforderlich die SSL-Anschlußnummer. Der Standard-SSL-Anschluß für das HTTPS-Protokoll ist Anschluß 443.
- Setzen Sie die SSL-Authentifizierungsoptionen (Client-Zulassung, Name und Kennwort und Anonym).

Mit Hilfe der SSL-Authentifizierungsoptionen können Sie die Zugriffsebene von Clients auf den Server einstellen. Sie können Client-Zulassung- oder grundlegende Kennwortauthentifizierung von Benutzern verlangen oder anonymen Zugriff auf den Server gestatten.

Verwandte Themen anzeigen

SSL-Client-Zulassungsauthentifizierung
Grundlegende SSL-Kennwortauthentifizierung
Anonymer SSL-Zugriff

### Grundlegende SSL-Kennwortauthentifizierung

Diese Methode verwendet ein grundlegendes Anfrage-/Antwort-Protokoll, um Namen und Kennwörter von Benutzern zu verlangen, und verifiziert dann die Übereinstimmung mit Kennwörtern, die im Sametime Adreßbuch gespeichert sind. Grundlegende Kennwortauthentifizierung mit SSL authentifiziert den Server und verschlüsselt Daten (einschließlich Benutzername und Kennwort), die zwischen Benutzer und Server übertragen werden.

Um grundlegende Kennwortauthentifizierung zu aktivieren, führen Sie folgende Aktionen aus:

- Legen Sie ein Personendokument an, und fügen Sie ein Internet-Kennwort hinzu.
- Wählen Sie im Abschnitt "Konfiguration der Internet-Anschlüsse und Sicherheit" des Serverdokuments in der Spalte für das Protokoll, für das Sie SSL aktivieren wollen, die Option "Nein" im Feld "Client-Zulassung" und "Ja" im Feld "Name und Kennwort".
- Richten Sie Datenbank-Zugriffskontrollisten (ACLs) ein.

### SSL-Client-Zulassungsauthentifizierung

Anhand dieser Methode kann der Server Clients basierend auf der SSL-Zulassung eines Benutzers authentifizieren. Zusätzlich zum Benutzer wird auch der Server authentifiziert und die zwischen Benutzer und Server übertragenen Daten werden verschlüsselt.

Nachstehende Anforderungen müssen erfüllt sein, bevor SSL-Client-Zulassungsauthentifizierung aktiviert werden kann:

- Der Client muß die Zulassungsstelle (CA), die die Server-Zulassung ausgestellt hat, als anerkanntes Root markieren.
- Der Server muß die CA, die die Client-Zulassung ausgestellt hat, in der Schlüsselringdatei des Servers als anerkanntes Root markieren.
- Der Client muß über eine Zulassung von einer internen oder externen CA verfügen.
- Für den Client muß ein Personendokument mit seiner öffentlichen Schlüsselzulassung im Sametime Adreßbuch vorhanden sein.

Führen Sie die folgenden Aktionen aus, um Client-Zulassungsauthentifizierung zu aktivieren:

- Wählen Sie im Abschnitt "Konfiguration für Internet-Anschlüsse und Sicherheit" des Serverdokuments in der Spalte für das Protokoll, für das Sie SSL aktivieren wollen, die Option "Ja" im Feld "Client-Zulassung".
- Richten Sie Datenbank-Zugriffskontrollisten (ACLs) ein.

## Anonymer SSL-Zugriff

Diese Methode authentifiziert den Server und verschlüsselt zwischen Benutzer und Server übertragene Daten, authentifiziert jedoch keine Benutzer. Verwenden Sie diese Methode nur, wenn Sie die Identität von Benutzern, die auf Ihren Server zugreifen, nicht kennen müssen.

Um anonymen Zugriff zu aktivieren, führen Sie folgende Aktionen aus:

Wählen Sie im Abschnitt "Konfiguration der Internet-Anschlüsse und Sicherheit" des Serverdokuments in der Spalte für das Protokoll, für das Sie SSL aktivieren wollen, die Option "Nein" im Feld "Client-Zulassung" und "Ja" im Feld "Anonym".

## Einrichten von Servern für automatische SSL-Verbindung von Clients

Sie können den Zugriff auf einen Server oder eine einzelne Datenbank so einrichten, daß nur diejenigen mit entsprechenden SSL-Zulassungen darauf zugreifen können. Clients, die eine Verbindung über TCP/IP aufbauen, erhalten keinen Zugriff.

SSL für alle Datenbanken auf einem Server erzwingen, der SSL verwendet:

1. Klicken Sie im Sametime Administrationswerkzeug auf "Server" und anschließend auf "Server".
2. Wählen Sie den Namen des Sametime Servers aus, um das Serverdokument zu öffnen.
3. Wählen Sie im Abschnitt "Konfiguration für Internet-Anschlüsse und Sicherheit" des Serverdokuments für das Protokoll, für das Sie SSL-Verbindungen erzwingen wollen, die Option "Redirect to SSL" im Feld "TCP/IP Anschlußstatus".

SSL für einzelne Datenbanken auf einem Server erzwingen, der SSL verwendet:

1. Klicken Sie im Lotus Notes Arbeitsbereich mit der rechten Maustaste auf die Datenbank, und wählen Sie "Eigenschaften: Datenbank".
2. Aktivieren Sie "Web-Zugriff: SSL-Verbindung anfordern" im Register "Allgemein".

## Einrichten von SSL für einen Internet- oder Intranet-Client

Sie können einen Internet- oder Intranet-Client so einrichten, daß er beim Zugriff auf einen Server Server-Authentifizierung, Nachrichtenvalidierung und Datenverschlüsselung verwendet. Sie können auch die Client-Authentifizierung verwenden, um die Identität eines Clients zu verifizieren.

Für den Zugriff auf einen Sametime Server mit Server-Authentifizierung, Nachrichtenvalidierung und Datenverschlüsselung muß der Benutzer:

- einen Client verwenden, z. B. einen Web-Browser, der den Einsatz von SSL unterstützt, und
- die Zulassungsstelle (CA), die diese Server-Zulassung ausgestellt hat, als anerkanntes Root markieren.
- Wenn der Server oder die Datenbank keine SSL-Verbindungen verlangt, muß der Client die korrekte Syntax verwenden, um eine sichere Transaktion zu initiieren. Folgendes Beispiel zeigt die korrekte Syntax für die Angabe der Server-URL, wenn ein Browser-Benutzer eine sichere Transaktion initiiert:

  `https://`

Wenn Client-Authentifizierung erforderlich ist, muß der Benutzer außerdem:

- über eine Client-Zulassung verfügen, die eine externe oder interne CA ausgestellt hat, und
- ein Personendokument im Sametime Adreßbuch besitzen, das eine öffentliche Schlüsselzulassung enthält.

Wenn Ihr Unternehmen eine interne CA verwendet, können Benutzer zur Anwendung "Zulassungsstelle" auf dem Sametime Server blättern und eine Client-Zulassung anfordern. Wenn die interne CA die Zulassungsanforderung genehmigt, teilt die Anwendung "Zulassungsstelle" in einer E-Mail eine URL mit, die angibt, wo die Zulassung abgeholt werden kann.

Die gängigsten Client-Softwareanwendungen umfassen Client-Zulassungen, die von anerkannten CAs, z. B. VeriSign, ausgestellt wurden. Wenn der Server eine Zulassung von einer dieser CAs besitzt, kann der Client automatisch eine Verbindung zum Server aufbauen, ohne die Server-Zulassung als anerkanntes Root zu markieren.

Verwandte Themen anzeigen

Anfordern einer Client-Zulassung für Client-Authentifizierung
Anzeigen und Verwalten von Zulassungsanforderungen
Unterzeichnen von Server-Zulassungen

### Anfordern einer Client-Zulassung für Client-Authentifizierung

Benutzer können wie folgt von einer internen CA eine Client-Zulassung zur Client-Authentifizierung anfordern:

1. Blättern Sie zur Anwendung "Zulassungsstelle".
2. Wenn Sie Microsoft Internet Explorer verwenden, bauen Sie eine TCP/IP-Verbindung zum Server auf. Internet Explorer erlaubt keine Übernahme von Site-Zulassungen in Ihren Browser.
3. Wenn Sie Netscape verwenden, sollten Sie eine Verbindung zur Anwendung "Zulassungsstelle" über SSL aufbauen. Wenn Sie der Browser zur Übernahme des Server-Zertifikats als vertrauenswürdige Root auffordert, akzeptieren Sie die Zulassung, indem Sie die Anleitungen des Browsers befolgen.
4. Klicken Sie im linken Fensterbereich auf "Client-Zulassung anfordern".
5. Geben Sie Ihren Namen und Firmeninformationen ein. Diese Informationen werden in Ihre Client-Zulassung aufgenommen.
6. Geben Sie zusätzliche Kontaktinformationen ein, die Sie an die CA senden wollen.
7. Wenn Sie Netscape Navigator verwenden, geben Sie die Schlüsselgröße für das Erzeugen des öffentlichen und des privaten Schlüssels an. Je größer der Schlüssel, um so stärker ist die Verschlüsselung.
8. Klicken Sie auf "Submit Certificate Request", um die Anforderung an die CA zu senden.

### Erstellen eines CA-Schlüsselrings und einer CA-Zulassung

Der Schlüsselring und die Zulassung der Zulassungsstelle (CA) ermöglicht Ihnen, Server- und Client-Zulassungen zu unterzeichnen, die Benutzern Zugang zu Ihrem Intranet gestatten. Um unbefugten Zugriff zu verhindern, bewahren Sie die CA-Schlüsselringdatei an einem sicheren Ort auf und erlauben nur bestimmten CA-Administratoren den Zugriff auf diese Datei.

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie "Zulassungsautorität öffnen" (CERTCA.NSF) über eine Netzwerkverbindung zum Server.
2. Klicken Sie auf "Zulassungsautoritäts-Schlüsselring & Zulassung erstellen".
3. Geben Sie einen Namen für die Schlüsselringdatei in das Feld "Name der Schlüsselringdatei" ein.
4. Geben Sie ein Kennwort in das Feld "Schlüsselringkennwort" ein, um den Inhalt der Schlüsselringdatei zu sichern.
5. Geben Sie den eindeutigen Namen des Servers ein.
6. Klicken Sie auf "Schlüsselring und Zulassung erstellen".
7. Wenn Sie die Information über die Schlüsselringdatei und den unterscheidbaren Servernamen gelesen haben, klicken Sie auf OK.
8. Legen Sie eine Sicherungskopie der CA-Schlüsselringdatei an, und speichern Sie sie an einem sicheren Ort.

Verwandte Themen anzeigen

Eindeutige Namen

### Details: Erstellen eines CA-Schlüsselrings und einer CA-Zulassung

- Der Standard-Dateiname der Schlüsselringdatei lautet CAKEY.KYR. Die Erweiterung .KYR sollte verwendet werden, damit Schlüsselring-Dateinamen konsistent sind.
- Wählen Sie den CA-Namen sorgfältig. Sobald Sie die CA-Zulassung erstellt haben und verwenden, ist es ein kostspieliges Verfahren, neue Zulassungen auszustellen, wenn Sie den CA-Namen ändern müssen.
- Sie können einen expliziten Pfad zur Schlüsselringdatei im Feld "Name der Schlüsselringdatei" angeben.
- Das Kennwort ist eine alphanumerische Zeichenfolge, die den Schlüsselring vor unbefugtem Zugriff schützt. Groß- und Kleinschreibung wird dabei unterschieden. Sie sollten mindestens sechs alphanumerische Zeichen für das Kennwort eingeben.
- Jede SSL-Zulassung enthält einen eindeutigen Namen, der von SSL-Transaktionen verwendet wird.
- Wenn Sie die Anwendung "Zulassungsstelle" von einer oder mehreren Workstations aus verwalten wollen, legen Sie Kopien der Schlüsselringdatei an und verteilen Sie diese auf die Workstations.

### Anzeigen und Verwalten von Zulassungsanforderungen

Als interne Zulassungsstelle (CA) können Sie Anforderungen ansehen, die auf Genehmigung oder auf ihre Abholung warten oder die Sie abgelehnt haben.

1. Klicken Sie im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Zulassungsautorität öffnen".
2. Klicken Sie auf "Server-Zulassungsanforderungen" oder "Client-Zulassungsanforderungen".
3. Verwenden Sie die Symbole in der Aktionsleiste, um Anforderungen, die auf Genehmigung warten, genehmigte Anforderungen und abgelehnte Anforderungen anzuzeigen.

### Unterzeichnen von Server-Zulassungen

Sie sollten unbedingt mit Ihrer Unternehmenspolitik bezüglich der Unterzeichnung von Zulassungen vertraut sein. Unterzeichnen Sie nur Zulassungen für Clients, die sich an die Sicherheitspolitik Ihres Unternehmens halten. Um eine Zulassungsanforderung zu genehmigen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, daß ein Personendokument für den Client im Sametime Adreßbuch angelegt ist.
2. Klicken Sie im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Zulassungsautorität öffnen".
3. Klicken Sie im linken Fensterbereich auf "Client-Zulassungsanforderungen".
4. Öffnen Sie die Anforderung, die Sie unterzeichnen wollen.
5. Prüfen Sie die Benutzerinformation und den eindeutigen Namen. Stellen Sie sicher, daß diese Information mit der Sicherheitspolitik Ihres Unternehmens in Einklang steht.
6. Lassen Sie die Option "Zulassung im Sametime Adreßbuch registrieren" aktiviert, um den öffentlichen Schlüssel des Clients automatisch in das Personendokument zu übernehmen.
7. Geben Sie eine Gültigkeitsdauer ein. Für Kurzzeitprojekte sind 90 Tage üblich, für ständige Projekte können Sie mehrere Jahre eingeben.
8. Wenn Sie der Person nicht per E-Mail mitteilen wollen, daß sie die Zulassung abholen kann, deaktivieren Sie "Send a notification email to the requestor". Andernfalls sendet die Anwendung "Zulassungsstelle" eine E-Mail mit einer URL, die den Ort angibt, an dem die Zulassung abzuholen ist.
9. Klicken Sie auf "Bestätigen", und geben Sie das Kennwort für die CA-Schlüsselringdatei ein.

Sie lehnen eine Zulassungssanforderung wie folgt ab:

10. Klicken Sie im Administrationsfenster auf "Systemdatenbanken", und wählen Sie "Zulassungsautorität öffnen".

11. Klicken Sie im linken Fensterbereich auf "Client-Zulassungsanforderungen".
12. Öffnen Sie die Anforderung, die Sie ablehnen wollen.
13. Geben Sie einen Grund für die Ablehnung ein.
14. Wenn Sie die Person nicht per E-Mail benachrichtigen wollen, deaktivieren Sie "Send a notification email to the requestor". Andernfalls sendet die Anwendung "Zulassungsstelle" eine E-Mail mit der Ablehnung und dem Grund der Ablehnung.
15. Klicken Sie auf "Ablehnen".

### Ändern des Profils für die Anwendung "Zulassungsstelle"

Das Profil der Zulassungsstelle (CA) identifiziert die Schlüsselringdatei der CA und gibt den Servernamen für URLs an, die Server-Administratoren mitteilen, daß sie die Server-Zulassung abholen können.

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Zulassungsautorität öffnen" (CERTCA.NSF) über eine Netzwerkverbindung zum Server.
2. Klicken Sie auf "Zulassungsautoritätsprofil konfigurieren".
3. Geben Sie falls erforderlich den Namen der Schlüsselringdatei ein.
4. Geben Sie den Hostnamen oder die IP-Adresse des Servers ein.

   **Hinweis** Der Sametime Server verwendet diesen Namen beim Senden von E-Mails an Serveradministratoren, um ihnen den Ort der abholbereiten unterzeichneten Server-Zulassung mitzuteilen.
5. Speichern Sie das Profildokument.

### Ändern des Kennworts für den Zugriff auf die CA-Schlüsselringdatei

Sie können das Kennwort der Schlüsselringdatei der Zulassungsstelle ändern, das im Profildokument der Zulassungsstelle aufgelistet ist. Für ständige Sicherheit der Schlüsselringdatei wird ein regelmäßiges Ändern des Kennworts empfohlen.

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie "Zulassungsautorität öffnen".
2. Klicken Sie auf "Zulassungsautoritäts-Schlüsselring anzeigen".
3. Klicken Sie auf "CA-Schlüsselringkennwort ändern".
4. Geben Sie das alte Kennwort ein, und klicken Sie auf OK.
5. Geben Sie das neue Kennwort ein, und klicken Sie auf OK.

**Hinweis** Geben Sie mindestens zwölf alphanumerische Zeichen für das Kennwort ein, um einfaches Erraten des Kennworts durch andere Personen zu verhindern.

### Testen der SSL mit einer selbstbestätigten Zulassung

1. Sie können einen selbstbestätigten Schlüsselring anlegen, um an Ihrer Site SSL zu Testzwecken einzurichten. Diese Zulassung ist von keiner Zulassungsstelle (CA) ausgestellt.
2. Klicken Sie im Administrationsfenster am Server auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Server-Zulassungsadministration öffnen" (CERTSRV.NSF).
3. Klicken Sie auf "Schlüsselring mit selbstbestätigter Zulassung erstellen".
4. Geben Sie einen Namen und ein Kennwort für die Schlüsselringdatei in die Felder "Name der Schlüsselringdatei" bzw. "Schlüsselringkennwort" ein.
5. Geben Sie die Information für den eindeutigen Namen ein.
6. Klicken Sie auf "Schlüsselring mit selbstbestätigter Zulassung erstellen".

## Möglichkeiten zur Verwaltung von SSL-Server-Zulassungen

Folgendes ist möglich:

- Anzeigen der Zulassungen, die in der Schlüsselringdatei gespeichert sind
- Erneuern einer abgelaufenen Zulassung
- Anzeigen Ihrer Anforderungen für Server-Zulassungen
- Markieren oder Zurückweisen der Zulassung einer CA als anerkanntes Root
- Ändern des Kennworts für den Zugriff auf die Schlüsselringdatei

## Anzeigen Ihrer Server-Zulassungen

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Server-Zulassungsadministration öffnen" (CERTSRV.NSF).
2. Klicken Sie auf "Schlüsselringe anzeigen & bearbeiten".
3. Sehen Sie falls erforderlich Zulassungen in einer anderen Schlüsselringdatei an, geben Sie den Namen der Schlüsselringdatei ein, die die gewünschten Zulassungen enthält, und geben Sie das Kennwort ein.
4. Führen Sie eine der folgenden Aktionen aus:
    - Wenn Sie Ihre Server-Zulassung anzeigen möchten, wählen Sie ein Dokument in der Kategorie "Site-Zulassung" aus.
    - Wenn Sie die Zulassung eines anerkannten Roots sehen möchten, wählen Sie ein Dokument in der Kategorie "Zulassungsstellen" aus.

## Erneuern einer abgelaufenen Server-Zulassung

Wenn eine Zulassung abgelaufen ist, können Sie sie nicht mehr zur Kommunikation mit Servern und Clients verwenden.

1. Legen Sie eine neue Schlüsselringdatei an, und fordern Sie eine neue Zulassung von der Zulassungsstelle (CA) an.
2. Mischen Sie die Zulassung der CA als anerkanntes Root in die Schlüsselringdatei.
3. Mischen Sie die Server-Zulassung in die Schlüsselringdatei.

## Anzeigen von Anforderungen für Server-Zulassungen

Wenn Sie eine Zulassungsanforderung an eine CA senden, zeichnet der Sametime Server folgende Information über die Anforderung auf:

- Methode für das Senden der Zulassung,
- Datum und Uhrzeit der Anforderung,
- Name der Schlüsselringdatei für die Zulassung,
- Information über die Zulassung,
- E-Mail-Adresse der CA, falls die Anforderung per E-Mail gesendet wurde.

Information über eine Zulassungsanforderung anzeigen:

1. Klicken Sie im Administrationsfenster auf dem Server auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Server-Zulassungsadministration öffnen" (CERTSRV.NSF).
2. Klicken Sie auf "Zulassungsanforderungsprotokoll anzeigen".
3. Öffnen Sie das Anforderungsdokument.

### Markieren oder Zurückweisen der Zulassung einer CA als vertrauenswürdiges Root

Entfernen Sie die Zulassung einer Zulassungsstelle (CA) als vertrauenswürdiges Root, wenn Sie nicht mehr mit Servern und Clients kommunizieren wollen, deren Zulassungen von dieser CA unterzeichnet sind.

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Server-Zulassungsadministration öffnen" (CERTSRV.NSF).
2. Klicken Sie auf "Schlüsselringe anzeigen & bearbeiten".
3. Bearbeiten Sie falls erforderlich Zulassungen in einer anderen Schlüsselringdatei, indem Sie auf "Schlüsselring für Anzeige wählen" klicken und den Namen und das Kennwort der Schlüsselringdatei eingeben, die die zu bearbeitenden Zulassungen enthält.
4. Öffnen Sie in der Kategorie "Zulassungsstelle" das Dokument, das die zu bearbeitende Zulassung enthält.
5. Führen Sie eine der folgenden Aktionen aus:
   - Sie markieren eine Zulassung als anerkanntes Root, indem Sie auf "Diese Zulassung anerkennen" klicken.
   - Sie markieren eine Zulassung als nicht anerkanntes Root, indem Sie auf "Diese Zulassung nicht anerkennen" klicken.

   **Hinweis** Der Sametime Server markiert die Zulassung als nicht anerkannt, entfernt sie aber nicht aus der Datenbank. Wenn Sie eine Zulassung permanent aus der Schlüsselringdatei löschen wollen, klicken Sie auf "Löschen". Eine gelöschte Zulassung können Sie nicht wiederherstellen, sondern Sie müssen sie erneut als anerkanntes Root mischen.
6. Geben Sie das Kennwort für die Schlüsselringdatei ein.

### Ändern des Kennworts für den Zugriff auf die Schlüsselringdatei

1. Klicken Sie im Administrationsfenster unter "Server" auf "Systemdatenbanken", und wählen Sie am lokalen Rechner "Server-Zulassungsadministration öffnen" (CERTSRV.NSF).
2. Klicken Sie auf "Schlüsselringe anzeigen & bearbeiten".
3. Klicken Sie auf "Schlüsselringkennwort ändern".
4. Geben Sie den Namen der Schlüsselringdatei ein, und klicken Sie auf OK.
5. Geben Sie das aktuelle Kennwort ein, und klicken Sie auf OK.
6. Geben Sie das neue Kennwort ein, und klicken Sie auf OK.

   **Hinweis** Verwenden Sie mindestens zwölf alphanumerische Zeichen für das Kennwort, um einfaches Erraten des Kennworts durch andere Personen zu verhindern.

# Kapitel 13: Erläuterung des Serverdokumtents

## Administrationseinstellungen im Serverdokument

Das Serverdokument enthält viele Administrationseinstellungen für den Sametime Server. Die Standardeinstellungen auf dem Serverdokument sollten so ausgelegt sein, daß der Sametime Server unter normalen Umständen eingesetzt werden kann. Sie können diese Einstellungen jedoch benutzerdefiniert festlegen, falls erforderlich.

**Hinweis** Einige Einstellungen auf dem Serverdokument sind nur dann relevant, wenn Sie den Sametime Server mit Lotus Notes Clients und Domino Servern verwenden.

Das Serverdokument wird wie in der nachfolgenden Liste in verschiedene Abschnitte unterteilt. Wenn Sie weitere Informationen über die einzelnen Bereiche und die enthaltenen Administrationseinstellungen benötigen, klicken Sie auf den entsprechenden Bereich.

- Allgemein
- Information zum Serverstandort
- Netzwerkkonfiguration
- Proxy-Konfiguration
- Sicherheit
- Beschränkungen
- Agent-Verwalter
- Administrationsprozeß
- Web-Retriever-Administration - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht verwendet.)
- Internet-Anschluß und Sicherheits-Konfiguration
- HTTP-Server
- LDAP - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht verwendet.)
- NNTP - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht verwendet.)
- Sametime Server
- Internet Message Transfer Agent (SMTP MTA) - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht unterstützt.)
- X.400 Message Transfer Agent (X.400 MTA) - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht unterstützt.)
- cc:Mail Message Transfer Agent (cc:Mail MTA) - (Einstellungen in diesem Abschnitt werden von Sametime 1.5 nicht unterstützt.)

Verwandte Themen anzeigen
Zugreifen auf das Serverdokument

## Zugreifen auf das Serverdokument

Verwenden Sie das Sametime Administrationswerkzeug, um auf das Sametime Serverdokument zuzugreifen. Das Sametime Serverdokument enthält viele Sametime Server Administrationseinstellungen. Wenn Sie den Sametime Server in einer Domino Umgebung installiert haben, können Sie auch mit dem Notes Client auf das Serverdokument zugreifen.

So greifen Sie auf das Sametime Serverdokument zu:

1. Öffnen Sie das Sametime Administrationswerkzeug. (Wählen Sie "Server-Administration" auf der Seite "Willkommen bei Sametime", und geben Sie Namen und Kennwort des Administrators ein.)

2. Wählen Sie "Server" und anschließend noch einmal "Server".
3. Klicken Sie auf den Namen des Sametime Servers, um die Sametime Administrationseinstellungen im Serverdokument anzuzeigen.
4. Klicken Sie auf "Server bearbeiten", um eine Einstellung im Serverdokument zu ändern. Blättern Sie zur entsprechenden Einstellung und ändern Sie die Option.
5. Nachdem Sie Änderungen vorgenommen haben, klicken Sie im oberen Bereich des Serverdokuments auf "Speichern und Schließen", um Ihre Änderungen zu speichern.

Verwandte Themen anzeigen
Administrationseinstellungen im Serverdokument

## Der Abschnitt "Allgemein" des Serverdokuments

Der Abschnitt "Allgemein" des Serverdokuments enthält allgemeine Konfigurationseinstellungen für den Sametime Server, wie z. B. den Namen des Servers und der Domäne (oder Community).

**Hinweis** Alle Einstellungen, die im Abschnitt "Allgemein" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die allgemeinen Einstellungen umfassen:

**Servername**

Die Einstellung des Servernamens legt den hierarchischen Servernamen fest. Der Servername besteht aus zwei Teilen: einem Domänennamen (oder Community Name) und dem DNS-Host-Namen. Bei acme.sametime.com/Acme ist z. B. Acme der Domänenname (oder Community Name) und acme.sametime.com ist der DNS Host-Name. Der Domänenname und DNS-Host-Name werden während der Sametime Serverinstallation festgelegt. Benutzer, die auf den Server über das Internet zugreifen, können nur den DNS-Host-Namen eingeben, um auf den Server zuzugreifen (z. B. http://www.acme.sametime.com).

**Servertitel**

Der Servertitel ist optional.

**Domänenname (oder Community Name)**

Der Domänenname (oder Community Name) wird während des Sametime Konfigurationsprogramms festgelegt. Sametime Server, die sich in derselben Domäne befinden, nutzen gemeinsam dasselbe Adreßbuch oder Verzeichnis.

Wenn Sie Sametime als reinen Web-Server verwenden, besteht die Sametime Community aus der Benutzerliste, die im Sametime Adreßbuch gespeichert ist.

**Cluster-Name**

Der Sametime Server kann nicht als Mitglied eines Domino Clusters verwendet werden.

**Master-Adreßbuchname**

Die Einstellung des Master-Adreßbuchnamens ist nur zutreffend, wenn Sie den Sametime Server in eine Domino Domäne integriert und einen Adreßverzeichnis-Assistenten eingerichtet haben, um Benutzern zu ermöglichen, zu blättern und Namen aus dem Adreßbuch anderer Domänen auszuwählen.

Wenn Sie einen Adreßverzeichnis-Assistenten eingerichtet haben, können Sametime Connect Benutzer den Adreßverzeichnis-Assistenten verwenden, um zu blättern und Namen aus dem Adreßbuch anderer Domänen auszuwählen.

**Server-Versionsnummer**

Die Einstellung der Server-Versionsnummer wird nicht verwendet.

**Administratoren**

Das Feld "Administratoren" zeigt eine Liste von Teilnehmern an, die autorisiert sind, den Server zu verwalten. Ein Administrator muß in diesem Feld aufgelistet sein, um die entfernte Serverkonsole oder die Konsole auf dem Sametime Administrationswerkzeug zu verwenden.

**Ist das ein Sametime Server?**
Die Einstellung "Ist das ein Sametime Server?" identifiziert anderen Sametime Servern den Server als Sametime Server. Diese Einstellung sollte immer "Ja" lauten, auch wenn nur ein Sametime Server installiert ist.

Wenn mehrere Sametime Server in einer Domäne installiert sind, muß Community Services alle anderen Sametime Server kennen. Community Services überprüft dieses Feld, um eine Liste von Sametime Servern zu erstellen.

Wenn mehrere Sametime Server installiert sind, werden alle Sametime Server, die in der Domäne installiert sind, in der Liste "Einzuladende Server" in der Benutzeroberfläche des Besprechungszentrums angezeigt. Services für Besprechungen überprüft dieses Feld, um eine Liste von Sametime Servern in der Domäne zu erstellen. Wenn ein Sametime Server einen anderen zu einer Online-Besprechung einlädt, verwendet der einladende Server die Einstellung "Netzadresse" im Abschnitt "Netzwerkkonfiguration" des Serverdokuments, um den anderen Server zu lokalisieren.

Verwandte Themen anzeigen
Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Server-Arbeitsumgebungsinformation" des Serverdokuments

Der Abschnitt "Server-Arbeitsumgebungsinformation" des Serverdokuments enthält die Zeitzone und die Einstellungen der Sommerzeit für den Sametime Server. Diese Einstellungen werden unabhängig davon benötigt ob Sie Sametime als Web-Only-Server oder in eine Domino Umgebung installiert haben.

**Hinweis** Alle Einstellungen, die im Abschnitt "Server-Arbeitsumgebungsinformation" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die unterstützten Einstellungen "Standortinformation" werden nachfolgend beschrieben:

**Ortszeit**
Die Einstellungen "Lokale Zeitzone" legen die Zeitzone fest, in der der Sametime Server verwendet wird. Der Server verwendet diese Einstellung, um die aktuelle Zeit an diesem Standort in die aktuelle Zeit im Ausland umzurechnen.

**Sommerzeit**
Die Einstellungen "Sommerzeit" legen fest, ob die Sommerzeit in der Zeitzone, in der der Server verwendet wird, beachtet oder nicht beachtet wird. Der Server verwendet diese Einstellung, um die aktuelle Zeit an diesem Standort in die aktuelle Zeit im Ausland umzurechnen.

Wenn Sie "Sommerzeit wird hier überwacht" auswählen, paßt der Server die Systemzeit automatisch an, wenn die Sommerzeit gilt.

Verwandte Themen anzeigen
Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Abschnitt "Netzwerkkonfiguration" des Serverdokuments

Der Abschnitt "Netzwerkkonfiguration" des Serverdokuments beinhaltet den Namen des Anschlusses, der vom Sametime Server verwendet wird, den Netzwerknamen, die Netzwerkadresse für den Sametime Server und eine Einstellung, um den Anschluß zu aktivieren oder zu deaktivieren. Diese Einstellungen wurden während des Konfigurationsvorgangs von Sametime festgelegt.

Das Sametime Konfigurationsprogramm findet automatisch verfügbare Anschlüsse. Im allgemeinen benötigt der Sametime Server nur einen TCP/IP-Anschluß.

**Hinweis** Alle Einstellungen, die im Abschnitt "Netzwerkkonfiguration" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die Einstellungen der Netzwerkkonfiguration umfassen:

**Anschluß**

Der Name des Anschlusses, der für den Sametime Server während des Konfigurationsprogramms festgelegt wird. Der Anschlußname, der vom Sametime Server verwendet wird, sollte TCP/IP lauten. Der Eintrag "TCP/IP" wird während des Sametime Konfigurationsprogramms für diesen Anschluß erstellt.

**Notes Netzwerk**

Der Name des Netzwerks, auf das der Anschluß zugreifen kann. Der Standardeintrag, der während der Konfiguration erstellt wird, lautet TCP/IP-Netzwerk.

**Netzadresse**

Die Einstellung "Netzadresse" enthält die Netzwerkadresse des Server-Anschlusses. In einem TCP/IP-Netzwerk kann die "Netzadresse" der vollständige DNS-Name sein, wie z. B. Servername.acme.com, oder die IP-Adresse des Servers. Wenn Sametime in einer Domino Domäne mit anderen Servern verwendet wird, legt diese Adresse die Adresse fest, die andere Server verwenden, um auf diesen Server zuzugreifen. Wenn Sie in der Domino Domäne mehr als einen Sametime Server installiert haben, wird diese Adresse verwendet, wenn ein Sametime Server einen weiteren Sametime Server zu einer Online-Besprechung einlädt.

**Aktiviert**

Sie müssen die aktivierte Einstellung auswählen, um den Anschluß zu verwenden.

Verwandte Themen anzeigen
Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Proxy-Konfiguration" des Serverdokuments

Nur die Protokolle "Notes Remote Procedure Call" werden zur Kommunikation über einen Proxy-Server unterstützt. Sametime Funktionalität ist nicht verfügbar, wenn Sie einen Proxy-Server zwischen dem Sametime Server und Ihrer Firewall einsetzen. Wenden Sie sich an den Internet-Systemadministrator, bevor Sie diese Einstellungen vornehmen.

**Hinweis** Alle Einstellungen, die im Abschnitt "Proxy-Konfiguration" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

**HTTP-Proxy**

Wenn Sie von Sametime aus einen HTTP-Proxy-Server verwenden, um auf das Internet zuzugreifen, geben Sie den Domänennamen oder die IP-Adresse Ihres HTTP-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Im allgemeinen wird dieses Feld nur für Server benötigt, die vom lokalen Netzwerk Ihres Unternehmens aus ans Internet angeschlossen werden.

**FTP-Proxy**

Wenn Sie von Sametime aus einen FTP-Proxy-Server verwenden, um auf das Internet zuzugreifen, geben Sie den Domänennamen oder die IP-Adresse Ihres FTP-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Im allgemeinen wird dieses Feld nur für Server benötigt, die vom lokalen Netzwerk Ihres Unternehmens aus ans Internet angeschlossen werden.

**Gopher-Proxy**

Wenn Sie von Sametime aus einen Gopher-Proxy-Server verwenden, um auf das Internet zuzugreifen, geben Sie den Domänennamen oder die IP-Adresse Ihres Gopher-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Im allgemeinen wird dieses Feld nur für Server benötigt, die vom lokalen Netzwerk Ihres Unternehmens aus ans Internet angeschlossen werden.

**SSL Security-Proxy**

Wenn Sie von Sametime aus einen SSL-Proxy-Server verwenden, um auf das Internet zuzugreifen, geben Sie den Domänennamen oder die IP-Adresse Ihres SSL-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Im allgemeinen wird dieses Feld nur für Server benötigt, die vom lokalen Netzwerk Ihres Unternehmens aus ans Internet angeschlossen werden.

**Notes RPC-Proxy**

Wenn Sie von Sametime aus einen HTTP-Proxy-Server verwenden, um von diesem Server aus auf das Internet zuzugreifen, und Sie im Internet Notes Protokolle verwenden möchten (z. B. Replizierung), geben Sie hier den Domänennamen oder die IP-Adresse Ihres HTTP-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Diese Feld wird nur bei Servern des lokalen Netzwerks Ihres Unternehmens benötigt, die im Internet mit anderen Notes Servern kommunizieren möchten. Diese Funktion setzt voraus, daß Ihr HTTP-Proxy-Server die HTTP-Verbindungsmethode unterstützt.

**SOCKS-Proxy**

Wenn Sie von Sametime aus einen SOCKS-Proxy-Server verwenden, um auf das Internet zuzugreifen, geben Sie den Domänennamen oder die IP-Adresse Ihres SOCKS-Proxy-Servers in Form eines Host-Namens ein: Anschlußadresse. Im allgemeinen wird dieses Feld nur für Server benötigt, die vom lokalen Netzwerk Ihres Unternehmens aus ans Internet angeschlossen werden.

**Kein Proxy für diese Hosts und Domänen**

Wenn Sie einen Proxy-Server verwenden, um auf das Internet zuzugreifen, aber vermeiden möchten, daß auch dieser Server den Proxy verwendet, um zu Servern Ihres lokalen Netzwerks eine Verbindung herzustellen, geben Sie den Domänennamen, Host-Namen oder die IP-Adresse für die Server Ihres lokalen Netzwerks ein. Ein Sternchen (*) kann als Platzhalter verwendet werden. Folgende Einträge sind gültig (z. B. acme.com, server.acme.com, 139.42.94.219, *.acme.com). Alle Proxy-Server nutzen das Feld "Kein Proxy" gemeinsam. Im allgemeinen wird dieses Feld nur für Server des lokalen Netzwerks Ihres Unternehmens benötigt, die zum Internet durch einen Proxy und auch zu anderen Servern Ihres lokalen Netzwerks eine Verbindung aufbauen.

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Sicherheit" des Serverdokuments

Die Einstellungen im Abschnitt "Sicherheit" sind nur relevant, wenn Sie Sametime in einer Domino Umgebung installiert haben. Diese Einstellungen führen auf dem Sametime Server dieselben Funktionen aus wie auf einem Domino Server.

**Hinweis** Alle Einstellungen, die im Abschnitt "Sicherheit" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die Sicherheitseinstellungen werden nachfolgend beschrieben.

**Öffentliche Schlüssel von Notes mit denjenigen vergleichen, die im Adreßbuch gespeichert sind**

Sie können den Sametime Server so konfigurieren, daß Clients sich nur authentifizieren können, wenn die öffentlichen Schlüssel auf den Client-IDs mit den öffentlichen Schlüsseln, die im Adreßbuch gespeichert sind, übereinstimmen.

Durch diese Konfiguration kann unautorisierte Verwendung von IDs vermieden werden. Wenn ein Benutzer die öffentlichen Schlüssel auf der Benutzer-ID ändert, verhindert diese Funktion, daß eine unautorisierte Person mit der Original-ID und dem öffentlichen Schlüssel auf den Server zugreift. Diese Funktion verhindert auch, daß eine Person, die sich nicht im Adreßbuch befindet bzw. einem anderen Unternehmen angehört oder das Unternehmen verlassen hat, auf einen Server zugreift.

Um öffentliche Schlüssel von Notes und Domino mit denjenigen, die sich im Adreßbuch befinden, zu verifizieren, wählen Sie "Ja" im Feld "Öffentliche Schlüssel mit denjenigen vergleichen, die im Adreßbuch gespeichert sind".

**Anonyme Notes Verbindungen erlauben**

Sie können Notes Benutzern anonymen Zugriff auf einen Sametime Server gewähren. Dies ermöglicht Benutzern und Servern, auf den Server zuzugreifen, ohne dabei authentifiziert zu werden. Dies ist äußerst nützlich, um den allgemein öffentlichen Zugriff auf Server zu gewähren, für die die Öffentlichkeit keine Querzulassung besitzt. Wenn Benutzer zu einem Server eine Verbindung herstellen möchten, der auf anonymen Zugriff festgelegt ist, und der Server sie nicht authentifizieren kann, erhalten Sie eine Nachricht, daß sie gerade anonym auf den Server zugreifen.

Um Notes Benutzern zu erlauben, anonym auf den Server zuzugreifen, wählen Sie "Ja" im Feld "Anonyme Notes Verbindungen zulassen".

**Kennwörter von Notes IDs überprüfen**

Sie können die Kennwortprüfung aktivieren, so daß Notes Benutzer sich nur bei einem Server authentifizieren können, wenn Sie das korrekte Kennwort verwenden.

Wenn eine unautorisierte Person eine ID verwendet und deren Kennwort in Erfahrung bringt, kann der Eigentümer der ID die Kennwortprüfung benutzen, um das Kennwort zu ändern, und so zu vermeiden, daß diese Person das Kennwort weiterhin zur Server-Authentifizierung verwendet. Wenn die unautorisierte Person das nächste Mal versucht, auf den Server zuzugreifen, und dabei die ID mit dem alten Kennwort verwendet, prüft der Server das Kennwort und verweigert den Zugriff, da das eingegebene Kennwort nicht mit dem neuen Kennwort übereinstimmt. Ohne die Kennwortprüfung kann eine unautorisierte Person eine ID und ein Kennwort verwenden, auch wenn der Benutzer das Kennwort auf seiner Kopie der ID geändert hat, da das Kennwort die Datei erfolgreich entschlüsseln kann. Sie müssen die Kennwortprüfung auf dem Server und Personendokument aktivieren.

Um die Kennwortprüfung auf dem Serverdokument zu aktivieren, wählen Sie im Feld "Kennwörter von Notes IDs überprüfen" die Option "Aktiviert".

Um die Kennwortprüfung in Personendokumenten zu aktivieren, verwenden Sie das Administrationsfenster. Klicken Sie auf "Personen" und wählen Sie Personenansicht". Wählen Sie jedes einzelne Personendokument aus, anschließend "Aktionen" > "Kennwortfelder festlegen" und klicken Sie auf "Ja", wenn Sie aufgefordert werden fortzufahren. Wählen Sie anschließend "Kennwort prüfen", und klicken Sie dann auf "OK".

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Beschränkungen" des Serverdokuments

Die Einstellung "Server von einem Browser aus verwalten" im Abschnitt "Beschränkungen" ist für alle Administratoren der Sametime Server unabhängig davon relevant, ob Sie Sametime als reinen Web-Server konfiguriert oder den Sametime Server in eine Domino Umgebung installiert haben.

Die anderen Administrationseinstellungen im Abschnitt "Restrictions" sind nur dann relevant, wenn Sie den Sametime Server in einer Domino Umgebung verwenden. Diese Einstellungen führen auf einem Sametime Server dieselben Funktionen aus, wie auf einem Domino Server.

**Hinweis** Alle Einstellungen, die im Abschnitt "Beschränkungen" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die "Beschränkungen"-Einstellungen werden nachfolgend beschrieben.

**Serverzugriff nur Benutzern erlauben, die in diesem Adreßbuch gelistet sind**

Diese Einstellung erlaubt nur Benutzern, die im Adreßbuch aufgelistet sind, auf den Server zuzugreifen. Wenn Sie "Ja" auswählen, verweigern Sie den Zugriff auf alle Server, was auch für die Benutzer und Gruppen, die sich nicht im Adreßbuch befinden, zutrifft. Um allen beliebigen Servern den Zugriff auf den Server zu erlauben, fügen Sie deren Namen in das Feld "Serverzugriff" hinzu.

Wenn Sie "Nein" auswählen, können Benutzer, Server und Gruppen, die nicht im Adreßbuch aufgelistet sind, auf diesen Server zugreifen.

Diese Einstellung betrifft nicht Internet oder Intranet-Benutzer, die auf den Server zugreifen.

**Serverzugriff**

Die Einstellung "Serverzugriff" ermöglicht Ihnen, die Namen von Lotus Notes oder Domino Benutzern, Servern und Gruppen, denen Sie den Zugriff auf diesen Server garantieren möchten, einzugeben. Dieses Feld freizulassen, garantiert allen zertifizierten Benutzern und Servern Zugriff.

**Kein Serverzugriff**

Die Einstellung "Kein Serverzugriff" ermöglicht Ihnen, Lotus Notes Benutzern den Zugriff zu verweigern, die nicht mehr für Ihr Unternehmen arbeiten, jedoch ihre Benutzer-IDs behalten haben. Geben Sie die Benutzer-, Server- und Gruppennamen, die nicht auf den Server zugreifen sollen, ein.

**Neue Datenbanken erstellen**

Die Einstellung "Neue Datenbanken erstellen" ermöglicht Ihnen zu kontrollieren, welche Lotus Notes Benutzer auf einem Server Datenbanken erstellen können. Geben Sie im Feld "Neue Datenbanken erstellen" die Benutzer-, Server- und Gruppennamen ein, denen Sie erlauben möchten, auf dem Server neue Datenbanken zu erstellen.

**Repliken erstellen**

Die Einstellung "Repliken erstellen" ermöglicht Ihnen zu kontrollieren, welche Lotus Notes Benutzer und Domino Server auf einem Server Datenbankrepliken erstellen können. Geben Sie im Feld "Repliken erstellen" die Benutzer-, Server- und Gruppennamen ein, denen Sie erlauben möchten, auf dem Server Datenbankrepliken zu erstellen.

**Server von einem Browser aus verwalten**

Die Einstellung "Server von einem Browser aus verwalten" listet Benutzer auf, denen es erlaubt ist, das Sametime Administrationswerkzeug zu verwenden. Sie müssen in dieses Feld einen Personennamen eingeben, wenn Sie möchten, daß diese Person das Sametime Administrationswerkzeug verwenden kann.

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Agent-Verwalter" des Serverdokuments

Die Administrationseinstellungen im Abschnitt "Agent-Verwalter" des Serverdokuments sind nur relevant, wenn Sie sie in einer Domino Umgebung installiert haben. Diese Einstellungen führen auf einem Sametime Server dieselben Funktionen aus, wie auf einem Domino Server.

**Hinweis** Alle Einstellungen, die im Abschnitt "Agent-Verwalter" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die "Agent-Verwalter"-Einstellungen werden nachfolgend beschrieben.

**Persönliche Agenten ausführen**

Die Einstellung "Persönliche Agenten ausführen" listet Lotus Notes Benutzer auf, die auf dem Sametime Server persönliche Agenten verwenden können. Persönliche Agenten können nur von Benutzern verwendet werden, die den Agent erstellen. Wenn Sie das Feld leer lassen, können alle Benutzer Persönliche Agenten starten.

**Beschränkte LotusScript/Java-Agenten ausführen**

Die Einstellung "Beschränkte LotusScript/Java-Agenten ausführen" listet Lotus Notes Benutzer auf, die Zugriff auf einen eingeschränkten Satz von LotusScript Funktionen haben, um Agenten zu erstellen. Eine Liste ausgeschlossener LotusScript Befehle finden Sie in Kapitel 7 im Handbuch für Anwendungsentwickler.

**Unbeschränkte LotusScript/Java-Agenten ausführen**

Die Einstellung "Unbeschränkte LotusScript/Java-Agenten ausführen" listet Lotus Notes Benutzer auf, die unter Verwendung aller LotusScript Funktionen Agenten erstellen können, um Datenbanken und Server-Ressourcen zu manipulieren.

**Tag- und Nacht-Parameter**

Mit der Einstellung "Tag- und Nacht-Parameter" können Sie kontrollieren, wann Agenten verwendet werden. Standardmäßig wird die Tageszeit von 8:00 bis 20:00 Uhr festgelegt und die Nachtzeit 20:00 bis 8:00 Uhr. Nachts werden dem Agent-Verwalter mehr Systemressourcen reserviert. Wenn Sie komplexe LotusScript Agenten verwenden, sollten Sie sie eventuell nachts verwenden, wenn der Systembedarf niedriger ist und die Agenten schneller sind.

**Anzahl von gleichzeitigen Agent-Ausführungsfelder**

Die Einstellung "Anzahl von gleichzeitigen Agent-Ausführungsfelder" legt fest, wie viele Agenten gleichzeitig auf dem Server verwendet werden können. In einer Datenbank kann nur ein Agent gleichzeitig laufen, in verschiedenen Datenbanken können jedoch mehrere Agenten gleichzeitig auf demselben Server verwendet werden, je nachdem, wie viele Sie in diesem Feld festlegen. Der Standard entspricht 1 zur Tageszeit und 2 zur Nachtzeit. Wenn diese Werte erhöht werden, um dem Agent-Verwalter zusätzliche

Server-Ressourcen zu reservieren, stehen anderen Server-Prozessen weniger Ressourcen zur Verfügung.

**Maximale Agenten-Ausführungszeit**

Die Einstellung "Maximale Agenten-Ausführungszeit" legt fest, wieviel Zeit einem LotusScript Agent zur Verfügung steht, um die Ausführung abzuschließen. Der Standard entspricht für die Tageszeit 10 Minuten und für die Nachtzeit 15 Minuten. Wenn ein LotusScript Agent mehr Zeit benötigt, um mehrere Tasks auszuführen, beendet der Agent-Verwalter den Agent vor Abschluß der Tasks; hierfür müssen Sie eventuell den Wert erhöhen. Wenn Sie beispielsweise den Wert auf 60 Minuten erhöhen, werden große Mengen an Systemressourcen verbraucht, falls der Agent einen Code-Fehler enthält, der zu einer Endlosschleife führt.

**Max. % belegt vor Verzögerung**

Die Einstellung "Max. % belegt vor Verzögerung" legt die CPU-Abrufzeit fest, die der Agent-Verwalter verwenden kann, bevor eine automatische Verspätung eingeleitet wird. Der Standard für dieses Feld entspricht 25 % für die Tageszeit und 35 % für die Nachtzeit. Wenn die Ressourcen für den Agent-Verwalter erhöht werden, stehen anderen Servervorgängen weniger Ressourcen zur Verfügung.

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Der Abschnitt "Administrationsprozeß" des Serverdokuments

Die Administrationseinstellungen im Abschnitt "Administrationsprozeß" des Serverdokuments sind nur relevant, wenn Sie den Sametime Server in einer Domino Umgebung installiert haben. Diese Einstellungen führen auf einem Sametime Server dieselben Funktionen aus, wie auf einem Domino Server. Wir empfehlen nicht, den Sametime Server als administrativen Server in einer Domino Domäne zu verwenden.

Wenn Sie den Sametime Server mit Domino Servern verwenden und für die Domäne den Administrationsprozeß aktiviert haben, kann der Administrationsprozeß auf dem Sametime Server automatische administrative Tasks ausführen.

**Hinweis** Alle Einstellungen, die im Abschnitt "Administrationsprozeß" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die Einstellungen des Administrationsprozesses werden nachfolgend beschrieben.

**Maximale Zahl der Threads**

Die Einstellung "Maximale Zahl der Threads" legt die Anzahl von Threads fest, die der Administrationsprozeß verwendet, um Anforderungen zu verarbeiten. Der Administrationprozeß verwendet drei Threads, um Anforderungen zu verarbeiten. Wenn Ihr Server ein Multi-Prozessor-System ist, und Sie die Administrationsprozeß-Leistung steigern möchten, können Sie die Anzahl von Threads erhöhen.

**Intervall**

Die Einstellung "Intervall" prüft, wie oft der Administrationsprozeß verschiedene Arten von Anforderungen ausführt. Wenn dieses Feld leer ist, entspricht der Standard 60 Minuten.

**Ausführung von Anforderungen einmal täglich um**

Die Einstellung "Ausführung von Anforderungen einmal täglich um" prüft die Zeit, zu der der Administrationsprozeß im Adreßbuch Personendokumente aktualisiert. Wenn dieses Feld leer ist, werden die Personendokumente um 12:00 Uhr aktualisiert.

**Ausführungsbeginn am/Ausführungsbeginn um**

Wenn Sie Server- oder Gruppennamen ändern oder löschen, kann ein Administrationsserver die Felder "Autor" und "Leser" in seinen Datenbanken aktualisieren. Diese Einstellungen steuern, wann ein Server diesen Vorgang ausführt. Der Standard entspricht immer Sonntag 12:00 Uhr. Um diesen Standard zu ändern, wählen Sie einen anderen Tag oder andere Wochentage oder legen Sie eine andere Zeit fest.

## Der Abschnitt "Internet-Anschluß und Sicherheit" des Serverdokuments

Der Abschnitt "Internet-Anschluß und Sicherheitskonfiguration" des Serverdokuments enthält Zugriffseinstellungen für die TCP/IP- oder SSL-Anschlüsse, die vom HTTP-Server verwendet werden, sowie SSL-Konfigurationseinstellungen. Diese Einstellungen betreffen den Web-Bowser-Zugriff auf den Server vom Internet aus.

**Hinweis** Alle Einstellungen, die im Abschnitt "Internet-Anschluß und Sicherheitskonfiguration" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die Administrationseinstellungen für den Internet-Anschluß und die Sicherheitseinstellungen des Serverdokuments werden nachfolgend beschrieben.

**SSL-Schlüsseldatei**

Wenn Sie SSL-Sicherheit implementiert haben, sollte diese Einstellung den Namen des SSL-Schlüsselrings, den der Sametime Web-Server zur Verschlüsselung verwendet, festlegen. Der Standard entspricht keyfile.kyr.

**SSL-Protokollversion**

Wenn Sie SSL-Sicherheit implementiert haben, sollte diese Einstellung die SSL-Protokollversion festlegen, mit der Sie eine Verbindung herstellen möchten. Sie haben folgende Möglichkeiten:

- Nur V2.0 - Verwendet nur SSL V2.0 Handshake und Protokoll.
- V3.0 Handshake - Verwendet SSL V3.0 Handshake und vereinbartes Protokoll.
- Nur V3.0 - Verwendet nur SSL V3.0 Handshake und Protokoll.
- V3.0 mit V2.0 Handshake - Verwendet SSL V2.0 Handshake mit vereinbartem Protokoll.
- Vereinbart - SSL erlauben, Handshake und Protokoll festzulegen.

**Abgelaufene SSL-Zertifikate annehmen**

Wenn Sie SSL-Sicherheit implementiert haben, legt diese Einstellung fest, ob SSL abgelaufene Zertifikate annimmt. Wählen Sie "Ja", damit SSL entfernte Zertifikate, die abgelaufen sind, annehmen muß. Wählen Sie "Nein", um Ablaufdaten für Zertifikate festzulegen.

**TCP/IP-Anschlußnummer**

Diese Einstellung stellt diejenige TCP/IP-Anschlußnummer zur Verfügung, über die Web-Browser vom Internet aus auf den Sametime Server zugreifen. Der Sametime Server wartet an diesem Anschluß auf HTTP-Anforderungen vom Internet. Die Standardanschlußnummer für den HTTP-Web-Server entspricht 80. Die Standardanschlußnummer für den LDAP-Server ist Anschluß 389.

**TCP/IP-Anschlußstatus**

Wählen Sie "Aktiviert", um den Zugriff über den oben festgelegten TCP/IP-Anschluß zu erlauben. Wählen Sie "Deaktiviert", um den Zugriff über den TCP/IP-Anschluß nicht zu erlauben.

**Authentifizierungsoptionen (TCP/IP)**

Authentifizierungsoptionen legen fest, ob der Server Benutzer, die darauf zugreifen, authentifiziert oder ihnen erlaubt, anonym darauf zuzugreifen. Der Zugriff auf den Server wird darüber hinaus durch ACLs der individuellen Anwendungen und Datenbanken auf dem Server sowie durch die Einstellung "Maximum Internet Name and Password" einer Anwendung oder Datenbank gesteuert. Die Standardeinstellung ist für "Anonym" wie auch für "Namens- & Kennwortzugriff" "Ja".

Wenn Sie in den Einstellungen "Anonym" und "Name & Kennwort" jeweils die Option "Nein" auswählen, greifen Sie über den oben festgelegten TCP/IP-Anschluß auf den Server zu.

Wenn Sie in der Einstellung "Anonym" "Nein" auswählen und in der Einstellung "Name & Kennwort" "Ja", werden Benutzer, die auf den Server über den oben festgelegten TCP/IP-Anschluß zugegriffen haben, aufgefordert, einen Namen und ein Kennwort einzugeben, bevor Sie auf den Server zugreifen. Der Benutzer muß sein Internet-Kennwort eingeben, bevor er auf den Server zugreifen kann. Wenn ein Benutzer kein Kennwort eingibt, wird die Meldung "Authorization failure" angezeigt. Anonymen Benutzern wird nicht erlaubt, über den Anschluß, der für das TCP/IP-Protokoll festgelegt wurde, auf den Server zuzugreifen.

Wenn Sie in den Einstellungen "Anonym" und "Name & Kennwort" jeweils "Ja" auswählen, kann ein Benutzer anonym auf den Server zugreifen. Die Sicherheit wird durch die Einstellungen in der ACL jeder Anwendung und Datenbank auf dem Server kontrolliert. Ein Benutzer wird nur authentifiziert, wenn eine Anwendungs- oder Datenbank-ACL den anonymen Zugriff verbietet. Wenn z. B. ein Benutzer versucht, die Anwendung "Online-Besprechungszentrum" zu öffnen, die

Online-Besprechungszentrum-ACL jedoch den anonymen Zugriff nicht erlaubt, wird der Benutzer vom Server aufgefordert, einen gültigen Benutzernamen und ein gültiges Kennwort einzugeben. Der Benutzer gibt sein Internet-Kennwort ein, um auf das Online-Besprechungszentrum zuzugreifen, und legt die Zugriffsebene in der Besprechungszentrum-ACL fest. Wenn die Besprechungszentrum-ACL anonymen Zugriff erlaubt, kann ein Benutzer auf das Online-Besprechungszentrum zugreifen, ohne dabei ein Kennwort einzugeben. Der Benutzer legt die Zugriffsebene für anonyme Benutzer in der Besprechungszentrum-ACL fest.

Wenn Sie in der Einstellung "Anonym" "Ja" auswählen und in der Einstellung "Name & Kennwort" "Nein", werden Benutzer nicht authentifiziert, wenn sie auf den Server oder dessen Anwendungen bzw. Datenbanken zugreifen. Der Administrator kann zu jeder Anwendung oder Datenbank auf dem Server einen anonymen ACL-Eintrag hinzufügen und dem anonymen Eintrag eine Zugriffsebene zuweisen. Wenn es keinen anonymen Eintrag gibt, erhalten Benutzer für die Anwendung oder Datenbank die Standardzugriffsebene.

**SSL-Anschlußnummer**

Wenn Sie SSL verwenden, um Daten zu verschlüsseln und zu validieren bzw. Server und Client-Identitäten zu verifizieren, stellt diese Einstellung den SSL-Anschluß, über den Internet-Benutzer auf den Sametime Server zugreifen, zur Verfügung. Der Sametime Server wartet an diesem Anschluß auf SSL-Verbindungen. Die Standardanschlußnummer des HTTP-Web-Servers lautet 443. Die Standardanschlußnummer für den LDAP-Server lautet 636.

**SSL-Anschlußstatus**

Wählen Sie "Aktiviert", wenn Sie den Sametime Server so konfiguriert haben, SSL zu verwenden. Internet-Benutzer greifen auf den Server über die SSL-Anschlußnummer zu. Alle Daten, die den SSL-Anschluß passieren, sind verschlüsselt. Wählen Sie "Deaktiviert", wenn Sie SSL nicht verwenden, um Daten zu verschlüsseln, die zwischen dem Client und dem Sametime Server ausgetauscht werden.

**Authentifizierungsoptionen (SSL)**

SSL enthält die Option "Client Certificate authentication". Diese Option ermöglicht dem Server, Clients zu authentifizieren, die auf dem SSL-Zertifikat des Clients basieren.

Die Optionen "Name & Password" und "Anonyme Authentifizierung" für SSL werden auf die gleiche Weise verwendet, wie die Optionen "Name & Kennwort" und "Anonym" für TCP/IP, die oben in diesem Abschnitt beschrieben werden.

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument
Einrichten von SSL auf einem Server

## Der Abschnitt "HTTP" des Serverdokuments

Hypertext Transfer Protocol (HTTP) ist das Standard-Internetprotokoll, durch das Web-Clients mit Web-Servern sprechen können. Der Sametime HTTP-Server ermöglicht Web-Browsern mit dem Sametime Server zu "sprechen". Der HTTP-Server wird während des Sametime Konfigurationsprogramms automatisch gestartet. Der Abschnitt "HTTP-Server" im Sametime Serverdokument enthält die folgenden Gruppeneinstellungen, die mit dem Sametime HTTP-Server in Verbindung stehen.

- Allgemein
- Zuordnung
- Festplatten-Cache für Bilder und Dateien
- Speicher-Caches
- Protokollierung aktivieren für
- Protokolldateieinstellungen
- Protokolldateinamen

- Vom Protokoll ausschließen
- Zeitlimits
- Zeichensatz-Zuweisung
- Konvertierung/Anzeige

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Die Einstellungen "Allgemein" für den HTTP-Server

Diese Einstellungen sind im Abschnitt "HTTP Server" des Serverdokuments enthalten.

**Hinweis** Alle "Allgemein"-Einstellungen, die im Abschnitt "HTTP-Server" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Die "Allgemein"-Einstellungen für den HTTP-Server sind die folgenden:

**Host-Name**

Die Einstellung "Host-Name" enthält den vollständigen Domänennamen des Geräts, auf dem Sie Sametime installiert haben. Um einen Alias zu verwenden, spezifizieren Sie einen beliebigen vollständigen Domänennamen, der für Ihr Gerät in Ihrem Domänennamen-Service (DNS) festgelegt ist.

Der Host-Name, den Sie festlegen, ist der Name, der an den Browser zurückgegeben wird. Wenn Ihr Gerät über keinen Host-Namen verfügt, der in einem DNS registriert ist, geben Sie im Feld "Host-Name" die IP-Adresse des Geräts ein. Dies ermöglicht Web-Clients, die IP-Adresse Ihres Gerätes zu verwenden, um eine Verbindung herzustellen.

Wenn Sie das Feld "Host-Name" leer lassen, verwendet Sametime den Host-Namen, der im TCP/IP-Stack des Betriebssystems festgelegt wurde.

**Mit Host-Namen verknüpfen**

Die Einstellung "Mit Host-Namen verknüpfen" ermöglicht Ihnen, den DNS-Namen oder die IP-Adresse, die im Feld "Host-Name" festgelegt wird, mit dem Sametime HTTP-Server zu verknüpfen. Sie können beispielsweise im Feld "Host-Name" des Abschnitts "HTTP" (vorausgehend beschrieben) eine IP-Adresse für den HTTP-Server eingeben, die nicht mit der IP-Adresse des Sametime Servers übereinstimmt. Ein Client kann dann Anforderungen direkt an die HTTP-Server-Komponente des Sametime-Servers stellen, indem er die IP-Adresse des HTTP-Servers in einer Anforderung an den Sametime Server mit einschließt. Diese Option kann verwendet werden, wenn Sie Firewall-Tunneling aktivieren.

**DNS-Suche**

Wählen Sie "Aktiviert", damit Sametime den DNS-Hostnamen des angeforderten Clients nachschlägt. Der Wert, den Sie in diesem Feld auswählen, betrifft die Funktionsweise des Sametime Servers:

Leistung - Wenn Sie "Deaktiviert" auswählen, verwendet der Server keine Ressourcen, um den Host-Name-Lookup auszuführen. Hierdurch wird die Leistung des Sametime Servers verbessert.

Die Protokolldateien und Datenbanken - Die Protokolldateien und Datenbanken enthalten entweder IP-Adressen oder Hostnamen, je nachdem, was Sie auswählen. Wenn Sie "Deaktiviert" wählen, enthalten die Protokolldateien und Datenbanken IP-Adressen; wenn Sie "Aktiviert" wählen, enthalten die Protokolldateien und Datenbanken Hostnamen, die dem Gerät entsprechen, das vom Web-Client verwendet wird.

**Standard-Homepage**

Die Einstellung "Standard-Homepage" legt die HTML-Datei fest, die zuerst angezeigt wird, wenn Benutzer zuerst auf den Server zugreifen.

Dieses Feld wird normalerweise nicht auf einem Sametime Server verwendet. Im allgemeinen sollten Sie die Seite "Willkommen bei Sametime" anzeigen, wenn Benutzer auf den Server zugreifen. Die Seite "Willkommen bei Sametime" ist ein Lotus Notes Dokument und keine HTML-Datei. Um sicherzustellen, daß diese Seite angezeigt wird, wenn Benutzer auf den Server zugreifen, verwenden Sie die Standardeinstellung im Feld "Home-URL" unter "Zuordnungsgruppe" im Abschnitt "HTTP-Server".

**HTTP-Clients zum Suchen von Datenbanken zulassen**

Die Einstellung "HTTP-Clients zum Suchen von Datenbanken zulassen" legt fest, ob alle Benutzer eine Liste aller Anwendungen und Datenbanken auf dem Server sehen dürfen. Diese Einstellung ist standardmäßig "Nein", wenn Sie Sametime als reinen Web-Server installiert haben.

Benutzer können eine Liste aller Anwendungen und Datenbanken auf dem Server anzeigen, indem Sie den Befehl "?OpenServer" an die Sametime Server-URL anhängen.

Wenn für dieses Feld "Nein" festgelegt ist, können Web-Benutzer die Liste von Anwendungen und Datenbanken nicht sehen, sie können jedoch immer noch zu individuellen Anwendungen und Datenbanken, auf die sie Zugriff haben, blättern.

**Maximum an Anforderungen über eine Verbindung**

Die Einstellung "Maximum an Anforderungen über eine Verbindung" legt die Anzahl von Anforderungen fest, die ein Browser während einer einzigen Verbindung zu einem Server stellen kann. Diese Einstellung ermöglicht Browser-Benutzern, mehrere Anforderungen an den Server zu senden, ohne dabei auf eine Antwort der vorherigen Anforderung zu warten.

**Anzahl der aktiven Threads**

Die Einstellung "Anzahl der aktiven Threads" legt die Anzahl von Threads fest, die der HTTP-Server verarbeiten kann. Wenn die Anzahl aktiver Threads erreicht ist, hält der Sametime Server neue Anforderungen zurück, bis die andere Anforderung beendet ist und Threads verfügbar werden. Um so leistungsstärker Ihr Gerät ist, um so mehr Threads sollten Sie festlegen. Wenn Ihr Gerät zuviel Zeit auf Overhead-Tasks verwendet, wie z. B. auf das Auslagern von Speicher, legen Sie eine geringere Anzahl von Threads fest.

**Mindestzahl der aktiven Threads**

Dieses Feld wird nicht verwendet.

Verwandte Themen anzeigen

Zugreifen auf das Serverdokument
Die Einstellungen "Zuordnung" für den HTTP-Server

## Die Einstellungen "Festplatten-Cache für Bilder und Dateien" für den HTTP Server

Die Einstellungen "Festplatten-Cache für Bilder und Dateien" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Sametime verwendet zwei verschieden Caches, um Server-Ressourcen zu verwalten: Datei und Speicher. Das Datenträger-Cache für Abbildungs- und Dateieinstellungen hat Einfluß auf das Datei-Cache.

Um die Antwortzeit zu optimieren, speichert Sametime Abbildungen und Dateianhänge im Datei-Cache-Verzeichnis, das Sametime\cache (standardmäßig) lautet. Da es länger dauern kann, Bitmap-Abbildungen in ein Web-Abbildungsformat zu konvertieren, ermöglicht die gesonderte Verarbeitung der konvertierten Dateien auf der Festplatte Sametime, Inline-Abbildungen schneller zurückzugeben. Die Speicherung von Dateien im Cache verbessert auch die Serverantwortzeit.

Die Einstellungen "Festplatten-Cache für Bilder und Dateien" für den HTTP-Server werden nachfolgend beschrieben.

**Cache-Verzeichnis**

Die Einstellung "Cache-Verzeichnis" legt das Verzeichnis fest, in dem Bilddateien und Dateianhänge gespeichert werden. Wenn ein Benutzer eine Seite anfordert, die eine Abbildung enthält, speichert Sametime die Abbildung im Cache-Verzeichnis. Wenn Sametime eine weitere Anforderung für dieselbe Seite erhält, zeigt es die im Cache-Verzeichnis gespeicherte Abbildung an, wodurch die Antwortzeit verkürzt wird. Wenn Sie im Feld "Cache-Verzeichnis" keinen vollständigen Pfad angeben, bezieht sich das Cache-Verzeichnis auf das Sametime Datenverzeichnis (C:\Sametime\data).

**Maximale Cache-Größe**

Die Einstellung "Maximale Cache-Größe" legt den maximal verfügbaren Speicherplatz in Megabyte (MB) für das Cache fest. Wenn Sie auf dem Server verfügbaren Speicherplatz haben, können Sie die maximale Cache-Standardgröße von 50 MB erhöhen. Im allgemeinen bleibt die Cache-Größe unterhalb der maximalen Größe, kann aber gelegentlich erhöht werden.

**Cache beim Herunterfahren löschen**

Die Einstellung "Cache beim Herunterfahren löschen" legt fest, ob Sametime den Cache automatisch löschen soll, wenn Sie den Server herunterfahren.

**Aufräumen**

Die Einstellung "Aufräumen" löscht Dateien aus dem Cache und beginnt mit der Datei, auf die am wenigsten zugegriffen wird. Wenn Sie "Caching" aktivieren, wird der Vorgang "Aufräumen" aktiviert, um zu vermeiden, daß der Cache die von Ihnen festgelegte maximale Größe überschreitet. "Aufräumen" entfernt Dateien, die nicht mehr gesondert verarbeitet werden sollen, und beginnt bei den Dateien, die am wenigsten verwendet werden. Der Vorgang "Aufräumen" läuft zu den in der Einstellung "Aufräumintervall" festgelegten Zeiten oder wenn die maximale Cache-Größe erreicht ist.

**Aufräumintervall**

Der Abschnitt "Aufräumintervall" legt ein Zeitintervall in Minuten fest, zu dem Sametime regelmäßig Cache-Dateien entfernt.

Verwandte Themen anzeigen
Zugreifen auf das Serverdokument

## Die Einstellungen "Speicher-Caches" für den HTTP-Server

Die Einstellungen "Speicher-Caches" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Sametime verwendet zwei Cache-Arten, um Serverressourcen zu verwalten: Datei und Speicher. Die Einstellungen "Speicher-Caches" beziehen sich auf den Speicher-Cache.

Um die Antwortzeit zu optimieren, verwendet Sametime Caches, um darin Speicherinformationen über HTTP-Befehle, Datenbanken und Benutzer zu speichern. Mapping-Information über Befehle und Datenbanken und die Authentifizierung von Benutzern können länger dauern. Der Speicher-Cache speichert diese Information im Speicher, so daß Sametime schnell darauf zugreifen kann.

Da der Cache im Speicher gespeichert wird, müssen Sie auf dem Server kein Verzeichnis angeben, um die Information zu speichern. Die Einstellungen "Speicher-Caches" für den HTTP-Server werden nachfolgend beschrieben.

**Maximum an gepufferten Befehlen**

Die Einstellung "Maximum an gepufferten Befehlen" legt die Anzahl an HTTP-Serverbefehlen fest, die für anonyme Benutzer gesondert verarbeitet werden sollen. Sametime muß einige HTTP-Serverbefehle in HTML konvertieren, bevor der Server die Befehle verarbeiten kann. Dieser Konvertierungsprozeß kann länger dauern. Verwenden Sie das Feld "Maximum an gepufferten Befehlen", um festzulegen, wie viele Befehle Sie im Speicher speichern möchten. Wenn ein Benutzer das nächste Mal einen Befehl ausführt, ist dieser sofort verfügbar.

**Maximum an gepufferten Gestaltungen**

Die Einstellung "Maximum an gepufferten Gestaltungen" legt die Anzahl von Lotus Notes Datenbank-Gestaltungselementen, die gesondert verarbeitet werden, für Benutzer fest. Die Online-Besprechungszentrum-Anwendung und andere Anwendungen und Datenbanken auf dem Server sind mit Lotus Notes entworfen. Für die Anzeige im Web-Client konvertiert der Sametime Server Notes Funktionen, wie z. B. Navigatoren, Ansichten, Dokumente, Verknüpfungen und andere Gestaltungselemente, automatisch in HTML.

Wenn ein Benutzer auf dem Server eine Anwendung oder Datenbank öffnet, muß Sametime einen Vorgang ausführen, der die Gestaltungselementnamen einer Identifikationsnummer zuordnet. Dieser Mapping-Vorgang kann länger dauern. Verwenden Sie das Feld "Maximum an gepufferten Datenbank-Gestaltungen", um festzulegen, wie viele Elemente Sie im Speicher speichern möchten. Wenn ein Benutzer das nächste Mal auf dieses Element zugreifen möchte, steht es sofort zur Verfügung.

**Maximum an gepufferten Benutzern**

Die Einstellung "Maximum an gepufferten Benutzern" legt die Anzahl von Benutzern fest, für die der Server den Namen, das Kennwort und die Gruppen, denen der Benutzer angehört, gesondert verarbeiten soll. Nachdem sich ein Benutzer erfolgreich bei einem Server authentifiziert hat, speichert Sametime den Benutzernamen, das Kennwort und die Liste von Gruppen, denen der Benutzer angehört, im Speicher. Verwenden Sie die Einstellung "Maximum an gepufferten Benutzern", um die Anzahl von Benutzern zu erhöhen, für die Sametime diese Information speichert. Sametime erstellt im Speicher einen Eintrag, um zu jedem Benutzer Informationen zu speichern. Sie sollten den Cache für einen Benutzer in periodischen Abständen löschen. Verwenden Sie das Feld "Ablauf", um einen Benutzer zu verpflichten, sich erneut zu authentifizieren.

**Ablaufintervall für gepufferte Benutzer**

Die Einstellung "Ablaufintervall für gepufferte Benutzer" legt die Zeitintervalle in Sekunden fest, in denen Sametime in regelmäßigen Abständen Benutzernamen, Kennwörter und Gruppenmitgliedschaften aus dem Cache entfernt.

Verwandte Themen anzeigen

Zugreifen auf das Serverdokument

Die Einstellungen "Festplatten-Cache für Bilder und Dateien" für den HTTP Server

## Die Einstellungen "Zeitlimits" für den HTTP-Server

Diese Einstellungen sind im Abschnitt "HTTP" des Serverdokuments enthalten. Die Einstellungen "Zeitlimits" legen Zeitbegrenzungen für Aktivitäten zwischen dem Sametime HTTP-Server und Clients oder CGI-Programmen fest.

Die Einstellungen "Zeitlimits" für den HTTP-Server werden nachfolgend beschrieben.

**Eingabe-Zeitlimit**

Die Einstellung "Eingabe-Zeitlimit" wird nicht verwendet, wenn Clients unter Verwendung der empfohlenen Web-Browser zum Sametime Server eine Verbindung herstellen. Die Einstellung "Eingabe-Zeitlimit" legt die Zeit in Minuten fest, innerhalb der der Client im Feld "Eingabe-Zeitlimit" eine Anforderung senden muß, nachdem er zum Server eine Verbindung aufgebaut hat. Der Server verwendet das Feld "Eingabe-Zeitlimit", wenn der Client, der mit dem Server verbunden ist, innerhalb der festgelegten Zeit "Header aktive lassen" nicht an den Server sendet. Die empfohlenen Browser senden "Header aktive lassen".

**Ausgabe-Zeitlimit**

Die Einstellung "Ausgabe-Zeitlimit" legt die maximale Zeit in Minuten fest, in der der Server an den Client im Feld "Ausgabe-Zeitlimit" eine "Ausgabe" senden muß. Das "Ausgabe-Zeitlimit" gilt für lokale Dateien und Anforderungen. Wenn der Server die vollständige Anforderung nicht innerhalb der im Feld "Ausgabe-Zeitlimit" festgelegten Zeit sendet, beendet der Server die Verbindung.

**CGI-Zeitlimit**

Die Einstellung "CGI-Zeitlimit" wird im allgemeinen nicht verwendet, da die Anwendungen und Datenbanken auf dem Sametime Server keine CGI-Programme verwenden. Diese Einstellung legt im Feld "CGI-Zeitlimit" die maximale Zeit in Minuten fest, in der ein CGI-Programm, das vom Server gestartet wurde, beendet sein muß. Wenn die Zeit, die im Feld "CGI-Zeitlimit" festgelegt wurde, ausläuft, sendet der Server an das CGI-Programm eine Meldung. Nach fünf Minuten schließt der Server ein Programm.

**Zeitlimit für ungenutzte Threads**

Diese Einstellung wird nicht verwendet.

Verwandte Themen anzeigen
Zugreifen auf das Serverdokument

## Die Einstellungen "Konvertierung/Anzeige" für den HTTP-Server

Diese Einstellungen sind im Abschnitt "HTTP" des Serverdokuments enthalten. Die Einstellungen "Konvertierung/Anzeige" prüfen das Format und die Methode, die Sametime verwendet, um Abbildungen anzuzeigen.

Die Einstellungen "Konvertierung/Anzeige" für den HTTP-Server werden nachfolgend beschrieben.

**Bildkonvertierungsformat**

Die Einstellung "Bildkonvertierungsformat" prüft das Dateiformat, das Sametime verwendet, wenn Abbildungen in der Anwendung des Online-Besprechungszentrums und andere Anwendungen und Datenbanken auf dem Sametime Server konvertiert werden. Die verfügbaren Formate sind GIF (Standard) und JPEG.

**Interlaced-Wiedergabe**

Die Einstellung "Interlaced-Wiedergabe" wird nur verwendet, wenn Sie als Abbildungskonvertierungsformat GIF ausgewählt haben. Wählen Sie im Feld "Interlaced-Wiedergabe" "Aktiviert" oder "Deaktiviert", um festzulegen, ob der Browser die GIF-Abbildung auf einmal oder jede Linie einzeln anzeigen soll.

**Progressive Darstellung**

Die Einstellung "Progressive Darstellung" wird nur verwendet, wenn Sie als Abbildungskonvertierungsformat JPEG ausgewählt haben. Wählen Sie im Feld "PProgressive Darstellung" "Aktiviert" oder "Deaktiviert", um festzulegen, ob der Browser die ganze Abbildung auf einmal oder auszugsweise in mehreren Schritten anzeigen soll.

**Hinweis** Wenn Sie "Progressive Darstellung" oder "Interlaced-Wiedergabe" aktivieren, hat der Benutzer das Gefühl, daß die Grafik schnell heruntergeladen wird, da das Bild identifiziert werden kann, bevor es vollständig heruntergeladen ist.

**JPEG-Bildqualität**

Die Einstellung "JPEG-Bildqualität" betrifft die Abbildungsqualität und Übertragungsdauer, wenn Sie als Abbildungskonvertierungsformat JPEG ausgewählt haben. Legen Sie für die JPEG-Abbildungsqualität einen Prozentwert zwischen 5 und 100 % fest. Je höher der Wert, umso größer ist die Datei und umso besser ist die Abbildungsqualität. Je niedriger der Wert ist, umso kleiner ist die Datei, umso kürzer die Übertragungsdauer und umso geringer die Abbildungsqualität.

**Maximale Zeilen pro Ansichtsseite**

Die Einstellung "Maximale Zeilen pro Ansichtsseite" prüft die Linienanzahl, die Sametime verwendet, um einem Benutzer eine Seite oder eine Ansicht in einer Notes Datenbank anzuzeigen.

**Vorgegebene Anzahl von Suchergebnissen**

Diese Einstellung wird nicht verwendet.

**Maximale Anzahl von Suchergebnissen**

Diese Einstellung wird nicht verwendet.

.

Verwandte Themen anzeigen

Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument

## Die Einstellungen "Zeichensatz-Zuweisung" für den HTTP-Server

Die Einstellungen "Zeichensatz-Zuweisung" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Sametime verwendet den Standardzeichensatz und die Zeichensatz-Mapping-Auswahl, um für den Browser HTML-Text zu generieren. Wenn Sie internationale Benutzer haben, die Text in anderen als den westlichen Sprachen lesen möchten, müssen Sie an den Einstellungen Änderungen vornehmen.

Die Einstellungen "Zeichensatz-Zuweisung" für den HTTP-Server werden nachfolgend beschrieben.

**Zeichensatz-Zuweisung**

Die Einstellung "Vorgabe-Zeichensatzgruppe" stellt folgende Optionen zur Verfügung: Westeuropäisch, Mitteleuropäisch, Japanisch, Traditionelles Chinesisch, Vereinfachtes Chinesisch, Koreanisch, Kyrillisch, Griechisch, Türkisch, Thai, Baltisch oder Mehrsprachig ISO10646. Sie können auch "Mehrsprachig" wählen (Native Code Page), um Benutzern zu erlauben, den gewünschten Zeichensatz zu wählen, wenn sie ein Dokument erstellen oder bearbeiten.

Im Feld, das den Zeichensatznamen anzeigt, wählen Sie eine der verfügbaren Möglichkeiten für "Zeichensatz-Zuweisung". Bei Zeichensätzen, die mehrere Optionen haben, müssen Sie darüber hinaus auswählen, welcher Zeichensatz verwendet werden soll. Wenn Sie "Mehrsprachig" (Native Code Page) auswählen, wählen Sie für jede Sprachgruppe einen Zeichensatz.

| Zeichensätze | Standard-Mapping | Zuweisung-Möglichkeiten | Anmerkungen |
|---|---|---|---|
| Westeuropäisch | Latein 1(ISO-8859-1) | Latein 1(ISO-8859-1) | Dieser Satz enthält Windows und ANSI-Zeichen. |
| Mitteleuropäisch | Latein 2(ISO-8859-2) | Latein 2(ISO-8859-2)<br>CP1250 | |
| Japanisch | SJIS | SJIS<br>JIS(ISO-2022-JP)<br>EUC-JP | |
| Traditionelles Chinesisch | Big5 | Big5<br>EUC-TW | |
| Vereinfachtes Chinesisch | GB | GB | |
| Koreanisch | KSC5601(EUC-KR) | KSC5601(EUC-KR)<br>ISO-2022-KR | |

| | | |
|---|---|---|
| Kyrillisch | ISO-8859-5 | ISO-8859-5<br>CP1251<br>KOI8-R |
| Griechisch | ISO-8859-7 | ISO-8859-7 |
| Türkisch | Latin 3(ISO-8859-3) | Latin 3(ISO-8859-3) |
| Thai | CP874 | CP874 |
| Baltisch | Windows-1257 | Windows-1257 |
| Mehrsprachig (ISO10646) | UTF-8 | UTF-7<br>UTF-8 |

Verwandte Themen anzeigen
Zugreifen auf das Serverdokument

## Die Einstellungen "Zuordnung" für den HTTP-Server

Die Einstellungen "Zuordnung" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Die Einstellungen "Zuordnung" für den HTTP-Server prüfen die Standorte der HTML-, CGI- und Symboldateien für den Sametime Server.

Die Einstellungen "Zuordnung" für den HTTP-Server werden nachfolgend beschrieben.

**Home-URL**

Die Einstellung "Home-URL" steuert das Lotus Notes Dokument, das angezeigt wird, wenn ein Benutzer auf den Server zugreift. Die Datenbank der Seite "Willkommen bei Sametime" (STCenter.nsf) wird standardmäßig festgelegt.

**HTML-Verzeichnis**

Die Einstellung "HTML-Verzeichnis" legt das Verzeichnis fest, in dem Sametime nach HTML-Dateien sucht. Das Standardverzeichnis ist Sametime\html.

Wenn Sie für die HTML-Dateien einen Speicherort festlegen, ist das Verzeichnis, das Sie festlegen, relativ für das Sametime Verzeichnis, wenn Sie nicht den vollständigen Pfad angeben. Wenn Sie beispielsweise \html in das HTML-Verzeichnis eingeben, sucht Sametime im Sametime\html-Verzeichnis nach den HTML-Dateien.

**Symbolverzeichnis**

Die Einstellung "Symbolverzeichnis" legt das Verzeichnis fest, in dem Sametime nach Symbolen sucht.

Wenn Sie für die Symboldateien einen Speicherort angeben, ist das Verzeichnis, das Sie festlegen, relativ für das Sametime Verzeichnis, wenn Sie nicht den vollständigen Pfad angeben. Wenn Sie beispielsweise \icon in das HTML Verzeichnis eingeben, sucht Sametime im Sametime\icon-Verzeichnis nach den HTML-Dateien.

**Symbol-URL-Pfad**

Die Einstellung "Symbol-URL-Pfad" legt den URL-Pfad für das Symbolverzeichnis fest. Im allgemeinen müssen Sie an der Einstellung "Symbol-URL-Pfad" nichts ändern.

**CGI-Verzeichnis**

Die Einstellung "CGI-Verzeichnis" legt das Verzeichnis fest, in dem der Server nach CGI-Programmdateien sucht.

**CGI-URL-Pfad**

Die Einstellung "CGI-URL-Pfad" legt den URL-Pfad für das CGI-Verzeichnis fest. Im allgemeinen müssen Sie an der Einstellung "CGI-URL-Pfad" nichts ändern.

Verwandte Themen anzeigen
Zugreifen auf das Serverdokument

## Die Einstellungen "Protokollierung aktivieren für" für den HTTP-Server

Die Einstellungen "Protokollierung aktivieren für" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Sametime sendet HTTP-Server-Protokollinformation an das Web-Serverprotokoll (DOMLOG.NSF). Sametime erstellt diese Datenbank automatisch, wenn Sie im Feld "Domlog.nsf" des Abschnitts "Protokollierung aktivieren für" "Datenbank-Protokollierung" aktivieren.

Sie können auch HTTP-Serverinformation an Textdateien protokollieren. Die Einstellungen "Protokollierung aktivieren für" für den HTTP-Server werden nachfolgend beschrieben.

**Protokolldateien**

Die Einstellung "Protokolldateien" ermöglicht Ihnen, HTTP-Server-Protokollinformationen in Textdateien zu speichern. Wählen Sie "Deaktiviert", wenn Sie die Protokollinformation nicht in Textdateien speichern möchten. Weitere Informationen hierzu finden Sie unter Info über die Einstellungen "Namen der Protokolldatein" für den HTTP Server.

**Domlog.nsf**

Die Einstellung "Domlog.nsf" ermöglicht Ihnen, Protokollinformationen an das Web-Serverprotokoll (DOMLOG.NSF) zu senden. Sametime erstellt diese Datei automatisch, wenn Sie in der Einstellung "Domlog.nsf" "Aktiviert" wählen.

Sie können die Einstellungen "Protokolldateien" und "Domlog.nsf" aktivieren, um die Protokollinformation im Web-Serverprotokoll und in Textdateien aufzuführen.

**Hinweis** Sie können das Sametime Administrationswerkzeug verwenden, um Information anzuzeigen, die in der Domlog.nsf-Datenbank enthalten ist. Öffnen Sie das Sametime Administrationswerkzeug, wählen Sie "Server" und anschließend "Web-Protokoll".

Verwandte Themen anzeigen

Die Einstellungen "Namen der Protokolldateien" für den HTTP-Server
Zugreifen auf das Serverdokument

## Die Einstellungen "Namen der Protokolldateien" für den HTTP-Server

Die Einstellungen "Namen der Protokolldateien" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Wenn Sie im Feld "Protokolldateien" des Abschnitts "HTTP" die Option "Protokoll" aktivieren, können Sie bis zu fünf verschiedene Dateien erstellen, um Sametime Web-Protokollinformation zu speichern.

Sametime startet jeden Tag eine neue Protokolldatei und hängt bei jeder HTTP-Anforderung Daten an die Dateien an. Sametime verwendet den Dateinamen, den Sie in den Einstellungen "Namen der Protokolldateien" festgelegt haben, und hängt ein Datensuffix an. Das Datensuffix entspricht dem Format *mmmddyy*, wobei *mmm* für die ersten drei Buchstaben des Monats steht, *dd* für den Monatstag und *yy* für die letzten zwei Jahreszahlen (beispielsweise agent_log.jul2198). Sametime erstellt um Mitternacht eine neue Protokolldatei, wenn der Server zu dieser Uhrzeit läuft. Wenn der Server um Mitternacht nicht läuft, startet Sametime eine neue Protokolldatei, wenn Sie am nächsten Tag den Server starten.

Um Speicherplatz zu sparen, prüfen Sie in periodischen Abständen die Größe der Protokolldateien, um sicherzustellen, daß diese nicht zu viel Platz einnehmen. Löschen Sie anschließend die Protokolldateien, die Sie nicht mehr benötigen.

Die Einstellungen "Namen der Protokolldateien" für den HTTP-Server werden nachfolgend beschrieben.

**Verzeichnis für Protokolldateien**

Die Einstellung "Verzeichnis für Protokolldateien" legt das Verzeichnis fest, in dem die Textprotokolldateien gespeichert werden. Wenn Sie dieses Feld leer lassen, werden Protokolldateien im Verzeichnis "Sametime\data" gespeichert.

**Zugriffsprotokoll**

Die Einstellung "Zugriffsprotokoll" protokolliert das Datum und die Zeit, zu denen die Anforderung gestellt wurde, die IP-Adresse des Benutzers (oder die DNS-Adresse, wenn "DNS-Suche" aktiviert ist), den Benutzernamen, wenn der Benutzer einen Namen und ein Kennwort angegeben hat, um auf den Server zuzugreifen, und den Statuscode, den der Server an den Browser zurücksendet, um anzuzeigen, ob die Anforderung erfolgreich oder nicht erfolgreich erstellt wurde.

Standardmäßig verzeichnet Sametime in diesem Protokoll einen Eintrag, sobald ein Client an den Server eine Anforderung sendet. Sie können die Einstellung "Vom Protokoll ausschließen" verwenden, um Anmeldeinformationen für bestimmte Clients zu überspringen. Der Standarddateiname ist ACCESS-LOG.

**Agent-Protokoll**

Die Einstellung "Agent-Protokoll" protokolliert das Datum und die Uhrzeit, zu der die Anforderung gestellt wurde, den verwendeten Browser-Typ, um auf den Server zuzugreifen, und den Statuscode, den der Server an den Browser zurücksendet, um anzuzeigen, ob die Anforderung erfolgreich oder nicht erfolgreich erstellt wurde. Der Standarddateiname ist AGENT-LOG.

**Fehlerprotokoll**

Die Einstellung "Fehlerprotokoll" protokolliert interne Server-Fehler. Der Standard-Servername ist ERROR-LOG.

**CGI-Fehlerprotokoll**

Die Einstellung "CGI-Fehlerprotokoll" protokolliert Standardfehler (stderr) von CGI-Programmen. Der Standarddateiname ist CGI-ERROR.

**Referenzprotokoll**

Die Einstellung "Referenzprotokoll" protokolliert das Datum und die Uhrzeit, zu denen die Anforderung gestellt wurde, die URL, die der Benutzer besucht, um Zugriff auf eine Seite zu erhalten, und den Statuscode, den der Server an den Browser zurücksendet, um anzuzeigen, ob die Anforderung erfolgreich oder nicht erfolgreich erstellt wurde. Der Standarddateiname lautet REFERER-LOG.

Verwandte Themen anzeigen

Die Einstellungen "Protokollierung aktivieren für" für den HTTP-Server
Die Einstellungen "Vom Protokoll ausschließen" für den HTTP-Server
Zugreifen auf das Serverdokument

## Die Einstellungen "Protokolldatei" für den HTTP-Server

Die Einstellungen "Protokolldatei" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Wenn Sie in der Einstellung "Protokolldateien" die Option "Protokoll" aktivieren, können Sie den Informationstyp steuern, der im Zugriffsprotokoll aufgeführt wird. Sie können auch festlegen, ob Anforderungen unter Lokalzeit oder Greenwicher Zeit (GMT) protokolliert werden. Die Einstellungen "Protokolldatei" für den HTTP-Server werden nachfolgend beschrieben.

**Zugriffsprotokollformat**

Die Einstellung "Zugriffsprotokollformat" steuert den Informationstyp, der im Zugriffsprotokoll aufgezeichnet wird. Wählen Sie "Allgemein", um nur Informationen, oder "Erweitert allgemein" um den Zugriff zu protokolliere. Weitere Informationen finden Sie in der Zugriffsprotokolldatei.

**Zeitformat**

Die Einstellung "Zeitformat" legt fest, ob Anforderungen nach Lokalzeit oder Greenwicher Zeit protokolliert werden. Wählen Sie "Lokal", um Anforderungen unter der Zeit zu protokollieren, die auf Ihrem System eingestellt ist, oder "GMT", um Anforderungen unter Greenwicher Zeit zu protokollieren.

Verwandte Themen anzeigen

Die Einstellungen "Protokollierung aktivieren für" für den HTTP-Server
Die Einstellungen "Namen der Protokolldateien" für den HTTP-Server
Zugreifen auf das Serverdokument

## Die Einstellungen "Vom Protokoll ausschließen" für den HTTP-Server

Die Einstellungen "Vom Protokoll ausschließen" sind im Abschnitt "HTTP" des Serverdokuments enthalten. Wenn Sie im Feld "Protokolldateien" des Abschnitts "HTTP" des Serverdokuments "Protokoll" aktivieren, können Sie für bestimmte HTTP-Anforderungstypen Protokolleinträge verhindern. Verwenden Sie die Einstellungen "Vom Protokoll ausschließen", um bestimmte HTTP-Anforderungstypen auszuschließen. Die Einstellungen "Vom Protokoll ausschließen" für den HTTP-Server werden nachfolgend beschrieben.

**URLs**

Die Einstellung "URLs" schließt bestimmte URL-Adressen aus dem Protokoll aus. Geben Sie eine URL-Adresse ein, die ausgeschlossen werden soll, z. B. *.gif.

**Verfahren**

Die Einstellung "Verfahren" schließt bestimmte HTTP-Methoden aus dem Protokoll aus. Geben Sie eine HTTP-Methode ein, die ausgeschlossen werden soll, z. B. POST oder DELETE.

**MIME-Typen**

Die Einstellung "MIME-Typen" schließt bestimmte MIME-Typen aus dem Protokoll aus. Geben Sie MIME-Typen ein, die ausgeschlossen werden sollen, z. B. image/gif.

**Benutzer-Agenten**

Die Einstellung "Benutzer-Agenten" schließt bestimmte Benutzer-Agenten aus dem Protokoll aus. Geben Sie die Benutzer-Agenten an, die ausgeschlossen werden sollen, z. B. Mozilla.

**Ausgabecodes**

Die Einstellung "Ausgabecodes" schließt bestimmte "Status-Ausgabecodes" aus dem Protokoll aus. Geben Sie die "Status-Ausgabecodes" ein, die ausgeschlossen werden sollen, z. B. 300.

**Hosts und Domänen**

Die Einstellung "Hosts und Domänen" schließt bestimmte Hosts und Domänen aus dem Protokoll aus. Geben Sie die Hosts und Domänen ein, die ausgeschlossen werden sollen, z. B. 130.333.* oder *.edu.

Um eine Host-Namen-Schablone im Feld "Auszuschließende Hosts und Domäne" einzugeben, müssen Sie die Einstellung "DNS-Suche" unter der Einstellung "Allgemein" im Abschnitt "HTTP" des Serverdokuments aktivieren. Wenn die Option "DNS-Suche" deaktiviert ist, können Sie nur IP-Adreßschablonen verwenden. Wenn z. B. die Einstellung "DNS-Suche" aktiviert ist, können Sie www.internotes.com;www.lotus.com;*.ibm.com verwenden; andernfalls müssen Sie eine IP-Adresse wie z. B. 192.168.*.* oder 192.168.77.* verwenden.

Verwandte Themen anzeigen

Die Einstellungen "Protokollierung aktivieren für" für den HTTP-Server
Zugreifen auf das Serverdokument

## Der Abschnitt "Sametime Server" des Serverdokuments

Die Administrationseinstellungen im Abschnitt "Sametime" des Serverdokuments sind im Serverdokument verfügbar und auch direkt vom Sametime Administrationswerkzeug aus zugänglich.

**Hinweis** Alle Einstellungen, die im Abschnitt "Sametime Server" des Serverdokuments erscheinen und nicht beschrieben sind, werden von Sametime 1.5 nicht verwendet.

Der Abschnitt "Sametime Server" des Sametime Serverdokuments enthält die folgenden Einstellungsgruppen für den Sametime Server.

- Community Server-Einstellungen
- Besprechungsserver-Einstellungen
- Protokoll-Einstellungen
- Community Server-Protokollierung
- Protokollierung aktivieren

- Besprechungsserver-Protokollierung
- Name des Textdatei-Protokolls

Verwandte Themen anzeigen
Administrationseinstellungen im Serverdokument
Zugreifen auf das Serverdokument
Sametime Überwachungs- und Protokollierungswerkzeuge

## Die Einstellungen "Community Server" für den Sametime Server

Die Einstellungen "Community Server" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit diesen Einstellungen können Sie Community Services so konfigurieren, daß sie mehrere Sametime Server unterstützen. Sie können auch festlegen, wie Community Services mit dem Adreßbuch interagiert.

Weitere Informationen über diese Einstellungen finden Sie unter Netzwerkeinstellungen für Community Services und Administrationseinstellungen für Community Services.

Verwandte Themen anzeigen
Der Abschnitt "Sametime Server" des Serverdokuments
Sametime Überwachungs- und Protokollierungswerkzeuge

## Die Einstellungen "Besprechungsserver" für den Sametime Server

Die Einstellungen "Besprechungsserver" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit diesen Einstellungen können Sie Netzwerkanschluß und Tunneling-Optionen festlegen.

Weitere Informationen finden Sie unter Netzwerkeinstellungen für Meeting Services und Administrationseinstellungen für Meeting Services.

Informationen über Serverbeschränkungen finden Sie im Abschnitt "Warnungen" unter "Zu protokollierende Besprechungsserver-Ereigniss" unter Festlegen der Protokollierungsparameter für das Sametime Protokoll.

Verwandte Themen anzeigen
Der Abschnitt "Sametime Server" des Serverdokuments
Sametime Überwachungs- und Protokollierungswerkzeuge

## Die Einstellungen "Protokoll" für den Sametime Server

Die Einstellungen "Protokoll" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit diesen Einstellungen können Sie den Dateityp des Sametime Protokolls, seinen Speicherort und die aufzuzeichnenden Ereignisarten von Community Services und Meeting Services festlegen.

Weitere Informationen finden Sie unter Festlegen von Protokollparametern für das Sametime Protokoll.

Verwandte Themen anzeigen
Der Abschnitt "Sametime Server" des Serverdokuments
Sametime Überwachungs- und Protokollierungswerkzeuge

### Community Server Protokolleinstellungen für den Sametime Server

Die Community Server Protokolleinstellungen befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit diesen Einstellungen können Sie wählen, welche Community Services Ereignisse in der Sametime Protokolldatenbank oder -datei aufgezeichnet werden sollen.

Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.

Verwandte Themen anzeigen
- Der Abschnitt "Sametime Server" des Serverdokuments
- Sametime Überwachungs- und Protokollierungswerkzeuge

### Die Einstellungen "Protokollierung aktivieren für" für den Sametime Server

Die Einstellungen "Protokollierung aktivieren für" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit diesen Einstellungen können Sie wählen, ob Sie Sametime Protokolldaten in der Sametime Protokolldatenbank oder einer Textdatei aufzeichnen wollen.

Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.

Verwandte Themen anzeigen
- Der Abschnitt "Sametime Server" des Serverdokuments
- Sametime Überwachungs- und Protokollierungswerkzeuge

### Die Einstellungen "Besprechungsserver-Protokollierung" für den Sametime Server

Die Einstellungen "Besprechungsserver-Protokollierung" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit Hilfe dieser Einstellungen können Sie Ereignisse protokollieren und Teilnehmer an Besprechungsdokumenten auflisten.

Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.

Verwandte Themen anzeigen
- Der Abschnitt "Sametime Server" des Serverdokuments
- Sametime Überwachungs- und Protokollierungswerkzeuge

### Die Einstellungen "Textdatei-Protokollname" für den Sametime Server

Die Einstellungen "Textdatei-Protokollname" befinden sich im Abschnitt "Sametime Server" des Serverdokuments. Mit Hilfe dieser Einstellung können Sie Speicherort und Name der Textdatei angeben. Geben Sie z. B. C:\SAMETIMELOG\STLOG.TXT ein, um die Sametime Information in der Datei stlog.txt im Verzeichnis Sametimelog auf der Server-Festplatte zu speichern. Wenn Sie das Feld "Pfad und Dateiname für das Sametime Protokoll" leer lassen, wird die Textdatei standardmäßig SAMETIME.LOG genannt.

Weitere Informationen finden Sie unter Festlegen der Protokollparameter für das Sametime Protokoll.

Verwandte Themen anzeigen
- Der Abschnitt "Sametime Server" des Serverdokuments
- Sametime Überwachungs- und Protokollierungswerkzeuge

# Kapitel 14: Verwenden Sametime-aktivierter Datenbanken auf einem Domino Server

## Verwenden Sametime-aktivierter Datenbanken

Der Sametime Server umfaßt Sametime Schablonen für Diskussionen und Beispiele für E-Mail und Dokumentbibliotheken, die Online-Awareness und Echtzeit-Chat-Funktionen mit häufig verwendeten Lotus Domino Datenbanken verbinden.

Datenbanken, die die Sametime-aktivierten Schablonen verwenden, zeigen die Listen "Wer ist anwesend" und "Wer ist online" an, die von Community Services auf dem Sametime Server unterstützt werden. Das Fenster "Wer ist online" listet Benutzer auf, die bei der Sametime Community angemeldet sind. Das Fenster "Wer ist anwesend" listet Benutzer auf, die dasselbe Dokument in einer Sametime Datenbank geöffnet haben.

Die Diskussionsschablone (STDISCUSS.NTF) wird komplett von Sametime 1.5 unterstützt. Ein Benutzer, der ein Dokument in einer Sametime Diskussion ansieht, kann die Option "Wer ist online" wählen, um eine Liste aller Online-Benutzer zu erhalten, die gerade das Dokument ansehen. Über die Option "An Chat hier teilnehmen" kann der Benutzer gemeinsam mit anderen Online-Benutzern an einer Echtzeitdisskussion des Dokuments teilnehmen, das sie ansehen. Mit Hilfe der Diskussionsschablone können Sie andere Sametime Diskussionsdatenbanken anlegen. Sie können auch das Design bestehender Diskussionsdatenbanken in der Domino Domäne ersetzen, um diesen Datenbanken Online-Awareness und Chat-Funktionen zur Verfügung zu stellen.

Die Dokumentbibliothek (STDOCLIB.NSF) und E-Mail- (STMAIL.NSF und STMAILW.NSF) Datenbanken sind Beispiele, die demonstrieren, wie Sie Sametime Funktionalität in neue Datenbanken einbinden können. Lotus Notes Entwickler sollten die Datenbank "Tools and Utilities" auf dem Sametime Server oder der Sametime Installations-CD ansehen, um Informationen zur Entwicklung von Sametime-aktivierten Datenbanken zu erhalten. Das Toolkit steht über eine Verknüpfung auf der Seite "Willkommen bei Sametime" oder im Verzeichnis /toolkit/index.html auf der CD zur Verfügung.

Sie können Sametime-aktivierte Datenbanken auf dem Sametime Server oder einem Domino Server in derselben Domäne einsetzen, in der Sametime installiert ist. Wenn Sie eine Diskussionsdatenbank auf einem Domino Server einsetzen, der Sametime nicht enthält, müssen Sie eine Reihe von Prozeduren ausführen, damit die Diskussionsdatenbank mit dem Sametime Community Server kommunizieren kann und Benutzer der Datenbank auf den Community Server zugreifen können. Weitere Informationen finden Sie unter Einsetzen Sametime-aktivierter Datenbanken auf Domino Servern.

## Einsetzen Sametime-aktivierter Datenbanken

Nach Installation eines Sametime Servers in einer Domino Umgebung können Sie Sametime-aktivierte Datenbanken auf anderen Servern in der Domäne einsetzen.

Der Sametime Server umfaßt eine Diskussionsschablone (STDISCUSS.NTF), über die Sie Online-Awareness und Chat-Funktionen in Diskussionsdatenbanken auf Domino Servern in der Domäne aufnehmen können. Verwenden Sie die Sametime Diskussionsschablone wie jede andere Domino Schablone, um auf Domino Servern neue Diskussionsdatenbanken anzulegen oder das Design bestehender Diskussionsdatenbanken zu ersetzen.

Der Sametime Server umfaßt zu Demonstrationszwecken auch Beispieldatenbanken für eine Dokumentbibliothek (STDOCLIB.NSF) und für E-Mail (STMAIL.NSF und STMAILW.NSF). Entwickler können anhand der Beispieldatenbanken auch lernen, wie Domino Anwendungen Sametime Funktionalität hinzugefügt wird.

Sie können eine Sametime Diskussionsdatenbank oder eine Beispiel-Dokumentbibliothek oder E-Mail-Datenbank auf einem beliebigen Server in der Domino Domäne verwenden. Sametime-aktivierte Datenbanken lassen sich auf folgenden Servern verwenden:

- Server, die Sametime und Domino enthalten, oder eigene Sametime Server, die als Teil einer Domino Domäne fungieren. (Ein eigener Sametime Server enthält Sametime, aber nicht Domino.) Weitere Informationen finden Sie unter Einsetzen Sametime-aktivierter Datenbanken auf Sametime Servern in einer Domino Domäne.
- Domino Server, die Sametime nicht enthalten. Weitere Informationen finden Sie unter Einsetzen Sametime-aktivierter Datenbanken auf einem Domino Server.

Wenn Sie eine Sametime E-Mail-Datenbank auf einem Domino Server einsetzen, können Sie für Benutzer der Beispiel-E-Mail-Datenbank Terminplanung einrichten.

Verwandte Themen anzeigen
Einsetzen Sametime-aktivierter Datenbanken auf Sametime Servern in einer Domino Domäne

## Einsetzen Sametime-aktivierter Datenbanken auf Sametime Servern in einer Domino Domäne

Sie können eine Datenbank für Sametime Diskussion, Dokumentbibliothek oder E-Mail auf einem Domino Server einsetzen, der Sametime enthält, oder auf einem eigenen Sametime Server, der Teil einer Domino Domäne ist.

Um eine Sametime-aktivierte Anwendung auf einem Domino Server einzusetzen, der Sametime enthält, legen Sie einfach mit Hilfe der Schablone STDISCUSS.NTF eine neue Diskussionsdatenbank an oder ersetzen Sie das Design einer bestehenden Diskussionsdatenbank auf dem Server, der Sametime enthält. Verwenden Sie für diese Aufgaben dieselben Prozeduren, die Sie für diese Aufgaben auf einem Domino Server ausführen würden.

Sobald die Sametime-aktivierte Datenbank auf dem Sametime Server vorhanden ist, müssen Sie den lokalen Server für die Mitglieder der Sametime Community festlegen. Weitere Informationen finden Sie unter Einrichten des lokalen Sametime Servers für Benutzer in der Sametime Community.

Verwandte Themen anzeigen
Einsetzen Sametime-aktivierter Datenbanken auf Domino Servern

## Einsetzen Sametime-aktivierter Datenbanken auf Domino Servern

Um eine Datenbank für Sametime Diskussion, Dokumentbibliothek oder E-Mail auf einem Domino Server einzusetzen, der Sametime nicht enthält, führen Sie die folgenden drei Prozeduren aus:

**Hinweis** Um Sametime-aktivierte Datenbanken auf einem Domino Server einzusetzen, müssen sich der Sametime Server und der Domino Server in derselben Domäne befinden. Diese Prozeduren lassen sich in beliebiger Reihenfolge ausführen.

1. Ändern Sie das Serverdokument des Domino Servers.
2. Erstellen Sie eine einmalige Replik der Datenbanken "Tokens" und "Secrets" auf dem Domino Server.
3. Legen Sie den lokalen Sametime Server für Benutzer in der Sametime Community fest.

Verwandte Themen anzeigen

Sametime-aktivierte Schablonen und Anwendungen
Ändern des Serverdokuments des Domino Servers
Erstellen einmaliger Repliken der Datenbanken "Tokens" und "Secrets" auf dem Domino Server
Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community

## Ändern des Serverdokuments des Domino Servers

Dies ist die erste von drei erforderlichen Prozeduren für den Einsatz von Sametime-aktivierten Datenbanken auf Domino Servern, die Sametime nicht enthalten, sich jedoch in derselben Domäne wie ein Sametime Server befinden. Datenbanken, die von einem Sametime Server auf einen Domino Server repliziert werden, enthalten Agenten, die von Sametime Development/Lotus Notes Companion Products signiert sind. Ändern Sie das Serverdokument des Domino Servers, um sicherzustellen, daß die Sametime-aktivierten Datenbanken von Sametime auf Domino repliziert werden können und daß die Agenten in den Sametime-aktivierten Datenbanken auf dem Domino Server laufen können.

Führen Sie im Notes Arbeitsbereich auf dem Domino Server folgende Aktionen durch:

1. Wählen Sie "Datei - Extras - Server-Administration".
2. Wählen Sie "Server - Serveransicht".
3. Doppelklicken Sie auf den Namen des Domino Servers. Das Serverdokument für den Domino Server wird geöffnet. Klicken Sie auf "Server bearbeiten", um das Serverdokument in den Bearbeitungsmodus zu bringen.
4. Blättern Sie zum Abschnitt "Beschränkungen" und wählen Sie "LocalDomainServers" im Feld "Repliken erstellen" aus. Klicken Sie auf "Hinzufügen" und dann auf OK. (Sie können auch den Namen des Sametime Servers in das Feld "Repliken erstellen" eingeben.)
5. Fügen Sie im Abschnitt "Agent-Manager" den Eintrag "Sametime Development/Lotus Notes Companion Products" in das Feld "Unbeschränkte LotusScript/Java-Agenten ausführen" ein.

   Fügen Sie auch etwaige andere Benutzer hinzu, die berechtigt sind, Sametime-aktivierte Datenbanken auf dem Domino Server anzulegen.
6. Klicken Sie auf "Speichern und Schließen", um diese Änderungen im Domino Serverdokument zu speichern.

Sobald Sie das Serverdokument für den Domino Server geändert haben, können Sie einmalige Repliken der Datenbanken "Tokens" und "Secrets" auf dem Domino Server erstellen.

Verwandte Themen anzeigen

Erstellen einmaliger Repliken der Datenbanken "Tokens" und "Secrets" auf dem Domino Server
Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community

## Erstellen einmaliger Repliken der Datenbanken "Tokens" und "Secrets" auf dem Domino Server

Dies ist die zweite von drei erforderlichen Prozeduren für den Einsatz von Sametime-aktivierten Datenbanken auf Domino Servern, die Sametime nicht enthalten. Um eine Sametime Diskussions-, Dokumentbibliotheks- oder E-Mail-Datenbank auf einem Domino Server einzusetzen, erstellen Sie eine einmalige Replik (oder "Teilreplik") der Datenbanken "Tokens" (STAuthT.nsf) und "Secrets" (STAuthS.nsf) auf diesem Domino Server. Die Datenbanken "Tokens" und "Secrets" authentifizieren gemeinsam Verbindungen von Sametime-aktivierten Datenbanken zu Community Services auf dem Sametime Server. Die Datenbank "Tokens" enthält auch einen Datensatz, mit dessen Hilfe die Community Services den lokalen Sametime Server eines Benutzers ermitteln können.

Führen Sie im Notes Arbeitsbereich auf dem Domino Server, auf dem Sie eine Sametime Datenbank einsetzen wollen, folgende Aktionen durch:

1. Stellen Sie sicher, daß keine Datenbanksymbole ausgewählt sind.
2. Wählen Sie "Datei - Replizierung - Neue Replik".
3. Wählen Sie den Sametime Server.
4. Geben Sie in das Feld für den Dateinamen "STAuthT.nsf" ein, um die Datenbank "Tokens" zu replizieren.
5. Klicken Sie auf die Schaltfläche "Öffnen". Das Dialogfeld "Neue Replik" wird geöffnet.
6. Wählen Sie im Bereich "Erstellen" die Option "Sofort" und stellen Sie sicher, daß das Feld "Zugriffskontrolliste kopieren" markiert ist.
7. Klicken Sie auf OK.
8. Wiederholen Sie diese Schritte, um eine einmalige Replik der Datenbank "Secrets" (STAuthS.nsf) auf jedem Domino Server anzulegen, auf dem Sie Sametime-aktivierte Datenbanken einsetzen wollen. (Geben Sie in Schritt 4 "STAuthS.nsf" anstelle von "STAuthT.nsf" ein.)

**Hinweis** Sie brauchen keinen Replizierungsplan für die Datenbanken "Secrets" und "Tokens" einzurichten, es sei denn, Sie wollen die Sicherheit für die Sametime-aktivierte Datenbank erhöhen. Weitere Informationen finden Sie unter Erhöhen der Sicherheit für Sametime-aktivierte Datenbanken

Sie können eine Sametime Datenbank auf einem beliebigen Domino Server einsetzen, auf dem Sie die Datenbanken "Secrets" und "Tokens" von einem Sametime Server repliziert haben und in dessen Serverdokument Sie die erforderlichen Einstellungen getroffen haben.

Nachdem Sie eine einmalige Replik der Datenbanken "Secrets" und "Tokens" angelegt haben, können Sie den lokalen Sametime Server für Benutzer in der Sametime Community festlegen.

Verwandte Themen anzeigen
Ändern des Serverdokuments des Domino Servers
Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community

## Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community

Diese Prozedur ist erforderlich, um Sametime-aktivierte Datenbanken auf einem Domino Server einzusetzen, der Sametime nicht enthält, oder auf einem Server, der Sametime enthält und als Teil einer Domino Domäne arbeitet.

Die Community Services unterstützen Online-Awareness und Chat-Funktionen von Sametime-aktivierten Datenbanken. Der "lokale" Server ist der Sametime Server, zu dem jeder Benutzer eine Verbindung aufbaut, wenn er Online-Awareness und Chat-Komponenten in Sametime Diskussions-, Dokumentbibliotheks- oder E-Mail-Datenbanken verwendet, die auf einem Domino Server eingesetzt werden. Wenn ein Benutzer auf die Sametime-aktivierte Datenbank zugreift, muß für diesen Benutzer eine Verbindung zu den Community Services auf einem Server, der Sametime enthält, aufgebaut werden.

Wenn Sie mehrere Sametime Server installieren, können Sie unterschiedliche lokale Server für Benutzer in der Sametime Community angeben. Weitere Informationen finden Sie unter Verwenden mehrerer Sametime Server .

Jedes Personendokument im Adreßbuch auf dem Sametime Server enthält das Feld "Sametime Server". Dieses Feld muß im Personendokument jedes Benutzers den Namen des Sametime Servers enthalten. Sie können einen einfachen Agent erstellen, um den Namen des Sametime Servers in das Feld "Sametime Server" im Personendokument jedes Benutzers einzugeben. Weitere Informationen über das Hinzufügen des Sametime Servernamens in Personendokumente finden Sie unter Details: Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community.

Wenn Sie die Sicherheit für Sametime-aktivierte Datenbanken auf Domino Servern erhöhen wollen, siehe Erhöhen der Sicherheit.

Verwandte Themen anzeigen

- Ändern des Serverdokuments des Domino Servers
- Erstellen einmaliger Repliken der Datenbanken "Tokens" und "Secrets" auf dem Domino Server

### Details: Festlegen des lokalen Sametime Servers für Benutzer in der Sametime Community

Wenn Sie einen Benutzer mit Hilfe des Sametime Administrationswerkzeugs hinzufügen, wird das Feld "Sametime Server" im Personendokument des Benutzers automatisch ausgefüllt. Das Feld enthält dann den Namen des Servers, auf dem das Sametime Administrationswerkzeug läuft.

Bei der Installation in einer Domino Umgebung, in der Domino Server in einer älteren Version als 4.6.5 läuft, wird das Adreßbuch nicht vom Sametime Server auf die Domino Server in der Domäne repliziert. Wenn Sie dem Adreßbuch auf dem Domino Server einen Benutzer hinzufügen und dieser durch Replizierung in das Adreßbuch auf dem Sametime Server eingefügt wird, müssen Sie den Namen des Sametime Servers manuell in das Personendokument auf dem Sametime Server eingeben oder einen entsprechenden Agent ausführen.

Wenn die Domino Server in Version 4.6.5 oder höher laufen, können Sie den Servernamen in das Personendokument auf dem Sametime Server oder auf dem Domino Server eingeben. Das Adreßbuch auf einem Domino Server 4.6.5 (oder höher) verfügt über alle Modifikationen, die zur Unterstützung eines Sametime Servers erforderlich sind, und läßt sich vom Sametime Server auf einen Domino Server replizieren.

### Erhöhen der Sicherheit für Sametime-aktivierte Datenbanken

Sie können beim Einsatz einer beliebigen Sametime Diskussions-, Dokumentbibliotheks- oder E-Mail-Datenbank deren Sicherheit erhöhen. Das Erhöhen der Sicherheit ist eine optionale Prozedur. Sie können die Sicherheit für Sametime-aktivierte Datenbanken erhöhen, die auf einem Server in einer Domino Domäne eingesetzt werden, einschließlich auf Servern, auf denen Sametime, Sametime und Domino oder nur Domino installiert ist. Das Erhöhen der Sicherheit bietet zusätzlichen Schutz vor unbefugten Benutzern, die auf den Sametime Server zugreifen wollen.

Verwandte Themen anzeigen

- Erhöhen der Sicherheit

## Erhöhen der Sicherheit

Dies ist eine optionale Prozedur, wenn Sie Sametime-aktivierte Datenbanken auf Servern einsetzen, die Sametime, Sametime und Domino oder nur Domino enthalten.

Sametime Server verwenden die Datenbank "Secrets" (STAuthS.nsf) beim Prozeß der Authentifizierung von Benutzern. Um höchste Sicherheit für Sametime-aktivierte Datenbanken zu erzielen, können Sie die Datenbank "Secrets" auf einem Sametime Server aktivieren, um Secrets zu generieren, und diese Secrets-Datenbank auf allen Servern in der Domäne replizieren, die eine Sametime-aktivierte Datenbank enthalten.

**Hinweis** Wenn Sie die folgenden Schritte an einem anderen als einem Sametime Server ausführen, müssen Sie über einen Agent "Beschränkt ausführen" und "Unbeschränkt ausführen" verfügen, der auf den Sametime Server zugreift. Andernfalls ist die Signierung des Agent und der Datenbank nicht korrekt und die Authentifizierung wird nicht problemlos ablaufen.

So erhöhen Sie die Sicherheit:

1. Aktivieren Sie den Agent zur Secrets-Generierung auf einem Sametime Server.
2. Replizieren Sie Secrets, um die Sicherheit für Sametime-aktivierte Datenbanken auf allen anderen Servern in der Domäne zu erhöhen.

Beachten Sie, daß Sie bei der Aktivierung des Agenten "SametimeSecretsGenerator" in einer Secrets-Datenbank diese Secrets-Datenbank auf allen Domino Servern replizieren müssen, auf denen Sametime-aktivierte Datenbanken eingesetzt werden.

Wenn mehrere Sametime Server in der Domäne installiert sind, müssen Sie auch die Secrets-Datenbank replizieren, in der der Agent "SametimeSecretsGenerator" für alle Server in der Domäne aktiviert ist, auf denen Sametime installiert ist.

Verwandte Themen anzeigen
Aktivieren des Agenten zur Secrets-Generierung auf einem Sametime Server
Replizieren von Secrets zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken

## Aktivieren des Agenten zur Secrets-Generierung auf einem Sametime Server

Dies ist die erste von zwei erforderlichen Prozeduren zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken, die auf Servern in der Domino Domäne installiert sind. Um die Sicherheit für Sametime-aktivierte Datenbanken auf Domino Servern zu erhöhen, müssen Sie den Agent SametimeSecretsGenerator auf einem Sametime Server aktivieren.

**Hinweis** Wenn Sie den Agent zur Secrets-Generierung auf einem anderen als einem Sametime Server aktivieren, müssen Sie über den Agent-Zugriff "Beschränkt ausführen" und "Unbeschränkt ausführen" auf den Sametime Server verfügen. Andernfalls ist die Signierung des Agent und der Datenbank nicht korrekt und die Authentifizierung wird nicht problemlos ablaufen.

So aktivieren Sie den Agent SametimeSecretsGenerator:

1. Öffnen Sie auf dem Sametime Server, der Secrets generieren wird, die Secrets-Datenbank (STAuthS.nsf).
2. Wählen Sie aus dem Menü "Ansicht" die Option "Agenten".
3. Klicken Sie in das Markierungsfeld links neben dem Agent SametimeSecretsGenerator. Stellen Sie sicher, daß "Lokal" ausgewählt ist. Klicken Sie auf OK.

Wenn Sie den Agent SametimeSecretsGenerator eingeschaltet haben, siehe Replizieren von Secrets zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken auf Domino Servern.

**Hinweis** Wenn nur ein Sametime Server in der Domäne installiert ist, ist keine weitere Prozedur für die Erhöhung der Sicherheit erforderlich.

Verwandte Themen anzeigen
Erhöhen der Sicherheit
Replizieren von Secrets zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken

## Replizieren von Secrets zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken

Dies ist die letzte von zwei erforderlichen Prozeduren zur Erhöhung der Sicherheit für Sametime-aktivierte Datenbanken.

Sie müssen ein Verbindungsdokument anlegen, das eine Ein-Weg-Replizierung von dem Sametime Server einrichtet, auf dem Sie den Agent SametimeSecretsGenerator für alle Server aktiviert haben, auf denen Sie Sametime-aktivierte Datenbanken einsetzen werden.

Es ist äußerst wichtig, die Secrets-Datenbank beim Anlegen des nachstehenden Verbindungsdokuments anzugeben. Andernfalls wird das für Sametime geänderte Adreßbuch auf den Domino Servern repliziert.

Führen Sie folgende Schritte im Lotus Notes Arbeitsbereich auf dem Server aus, auf dem die Secrets-Datenbank repliziert wird:

1. Öffnen Sie das Öffentliche Adreßbuch.
2. Wählen Sie die Verbindungsansicht und klicken Sie auf "Add Connection".

   Füllen Sie die korrekten Felder im Verbindungsdokument aus. In nachstehendem Beispiel enthält der Server "Boston01" die Sametime-aktivierte Datenbank und der Server "STBoston01" ist der Sametime Server, der die Secrets generiert. Die Server befinden sich in der ACME-Domäne.

   Beispiel für Verbindungsdokument:

   | | |
   |---|---|
   | Connection Type: | LAN |
   | Source Server: | Boston01/ACME (auf diesem Server liegt die Sametime-aktivierte Datenbank) |
   | Destination Server: | STBoston01/ACME (Server, der Secrets generiert) |
   | Source Domain: | ACME |
   | Destination Domain: | ACME |
   | Scheduled: | Enabled |
   | Tasks: | Replication |
   | Call Times: | 12:01 AM - 11:59 PM |
   | Repeat Interval | 180 Minutes |
   | Days: | Sun, Mon, Tues, Wed, Thu, Fri, Sat |
   | Replication Type: | Pull Only |
   | Files/Dir to Replicate | STAuthS.nsf |

3. Klicken Sie auf "Save and Close".
4. Wiederholen Sie den obigen Prozeß, um Verbindungdokumente anzulegen für die Replizierung zwischen dem Sametime Server (Boston01 im obigen Beispiel), der die Secrets generiert, und jedem Domino Server, auf dem Sametime-aktivierte Datenbanken eingesetzt werden sollen.
5. Schließen Sie das Öffentliche Adreßbuch.

Damit ist der Prozeß zur Erhöhung der Sicherheit für Sametime Datenbanken auf Domino Servern abgeschlossen.

Verwandte Themen anzeigen
Erhöhen der Sicherheit
Aktivieren des Agenten zur Secrets-Generierung auf einem Sametime Server

## Einrichten von Terminplanung für Sametime Beispiel-E-Mail-Datenbanken

Die Sametime Beispiel-E-Mail-Datenbank (STMAIL.NSF) umfaßt eine aktualisierte Komponente für Terminplanung. Mit Hilfe dieser Komponente kann ein Benutzer eine Besprechung im Online-Besprechungszentrum auf einem Sametime Server planen und automatisch Teilnehmer per E-Mail dazu einladen. Diese Funktion wird nur für Lotus Notes Clients unterstützt.

Nachdem Sie die Sametime Beispiel-E-Mail-Datenbank auf einen anderen Server in der Domäne zur Verfügung gestellt haben, können Sie die Sametime Funktionen zur Terminplanung einrichten. Hierzu gehören drei Prozeduren:

1. Ändern Sie die Einstellungen im Dokument "Mail-In-Datenbank hinzufügen" auf dem Domino Server.
2. Aktivieren Sie den Agent im Online-Besprechungszentrum.
3. Gestatten Sie Benutzern, Online-Besprechungen über die Terminplanung zu planen.

Verwandte Themen anzeigen

Ändern der Einstellungen im Dokument "Mail-In-Datenbank hinzufühen" auf dem Domino Server
Aktivieren des Agent für die Datenbank des Online-Besprechungszentrums (STConf.nsf) auf dem Sametime Server
Benutzern gestatten, Online-Besprechungen über die Terminplanung zu planen

## Ändern der Einstellungen im Dokument "Mail-In-Datenbank hinzufühen" auf dem Domino Server

Dies ist die erste von drei erforderlichen Prozeduren, um Lotus Notes Benutzern die Planung von Online-Besprechungen und das Einladen der Teilnehmer über die Terminplanungsfunktionen einer Sametime Beispiel-E-Mail-Datenbank zu erlauben. Sie müssen den Namen des Sametime Servers, die Sametime Server-Domäne und den Dateinamen des Online-Besprechungszentrums im Dokument "Mail-in-Datenbank hinzufügen" auf dem Domino Server eingeben.

Führen Sie im Notes Arbeitsbereich auf dem Domino Server folgende Aktionen durch:

1. Wählen Sie "Datei - Extras - Serveradministration".
2. Wählen Sie "Server - Serveransicht". Wählen Sie in der Server-Ansicht die Ansicht "Mail-In-Datenbanken und Ressourcen".
3. Klicken Sie auf die Aktionsschaltfläche "Dokument "Mail-In-Datenbank hinzufügen"".
4. Geben Sie den Namen des Sametime Servers in das Feld "Mail-In-Name" ein.
5. Geben Sie den Namen des Sametime Servers in das Feld "Server" ein.
6. Geben Sie die Domäne in das Feld "Domäne" ein.
7. Geben Sie "STConf.nsf" in das Feld "Dateiname" ein.
8. Speichern und schließen Sie das Dokument "Mail-In Database".

**Hinweis** Benutzer können Online-Besprechungen über den Kalender in der Mail-Datenbank planen. Wenn eine Besprechung über den Kalender eines Benutzers geplant wird, aktualisiert der Agent "AutoProcessReservations" im Online-Besprechungszentrum (STConf.nsf) die Besprechungsliste im Online-Besprechungszentrum. Der Agent-Manager auf dem Sametime Server steuert, wann dieser Agent abläuft. Da der Agent in festgelegten Intervallen abläuft, kann es bis zu 20 Minuten dauern, bevor im Kalender eines Benutzers geplante Besprechungen in der Besprechungsliste im Online-Besprechungszentrum erscheinen.

Nach Ändern der Einstellungen im Dokument "Mail-In-Datenbank hinzufügen" auf dem Domino Server, können Sie den Agent für die Anwendung "Besprechungszentrum" (STConf.nsf) auf dem Sametime Server aktivieren.

Verwandte Themen anzeigen

Einrichten von Terminplanung für Sametime Beispiel-E-Mail-Datenbanken
Aktivieren des Agent für die Datenbank des Online-Besprechungszentrums (STConf.nsf) auf dem Sametime Server
Benutzern gestatten, Online-Besprechungen über die Terminplanung zu planen

## Aktivieren des Agent für die Datenbank des Online-Besprechungszentrums (STConf.nsf) auf dem Sametime Server

Dies ist die zweite von drei erforderlichen Prozeduren, um Lotus Notes Benutzern die Planung von Online-Besprechungen und das Einladen von Teilnehmern über die Terminplanungsfunktionen einer Sametime Beispiel-E-Mail-Datenbank zu erlauben. In dieser Prozedur wird dem Agent AutoProcessReservations in der Datenbank des Online-Besprechungszentrums (STConf.nsf) die Fähigkeit verliehen, auf dem Sametime Server abzulaufen. Der Agent AutoProcessReservations aktualisiert die Besprechungsliste in der Datenbank des Online-Besprechungszentrums, wenn neue Besprechungen beginnen oder geplant werden.

Führen Sie im Notes Arbeitsbereich auf dem Sametime Server folgende Aktionen durch:

1. Wählen Sie "Datei - Datenbank - Öffnen".
2. Stellen Sie sicher, daß "Lokal" als Server gewählt ist.
3. Geben Sie "STConf.nsf" in das Feld "Dateiname" ein.
4. Klicken Sie auf "Symbol hinzufügen" und dann auf "Fertig".
5. Rechtsklicken Sie auf das Symbol und wählen Sie "Gehe zu Agenten".
6. Klicken Sie in das Markierungsfeld links neben dem Agent "AutoProcessReservations". Stellen Sie sicher, daß "Lokal" ausgewählt ist. Klicken Sie auf OK. (Neben dem Namen des Agent muß eine Markierung erscheinen.)
7. Schließen Sie die Ansicht "Agenten".

Nach Aktivieren des Agent für die Datenbank des Online-Besprechungszentrums auf dem Sametime Server können Sie Benutzern gestatten, Online-Besprechungen über die Terminplanung zu planen.

Verwandte Themen anzeigen

Einrichten von Terminplanung für Sametime Beispiel-E-Mail-Datenbanken
Ändern der Einstellungen im Dokument "Mail-In-Datenbank hinzufühen" auf dem Domino Server
Benutzern gestatten, Online-Besprechungen über die Terminplanung zu planen

## Benutzern gestatten, Online-Besprechungen über die Terminplanung zu planen

Dies ist die letzte von drei erforderlichen Prozeduren, um Benutzern von Lotus Notes die Planung von Online-Besprechungen und das Einladen von Teilnehmern über die Terminplanungsfunktionen einer Sametime Beispiel-E-Mail-Datenbank zu erlauben. Wenn Sie die Mail-Schablone auf einem Domino Server durch eine Sametime Mail-Schablone ersetzen, können Benutzer Online-Besprechungen über ihre Lotus Notes Kalender planen. Der Administrator muß jeden Benutzer anweisen, den Namen des Sametime Servers in sein Kalenderprofil einzugeben.

Um den Namen des Sametime Servers in das Kalenderprofil einzugeben, muß jeder Sametime Benutzer die folgenden Schritte ausführen:

1. Mail-Datenbank öffnen
2. Kalender-Ansicht wählen
3. "Aktionen - Kalenderwerkzeuge - Kalenderprofil" wählen
4. "Weitere Kalenderoptionen" öffnen
5. Im Bereich "Standardeinstellungen" den Namen des Sametime Servers in das Feld "Sametime Server" eingeben
6. Auf OK klicken

Verwandte Themen anzeigen

Einrichten von Terminplanung für Sametime Beispiel-E-Mail-Datenbanken
Ändern der Einstellungen im Dokument "Mail-In-Datenbank hinzufühen" auf dem Domino Server
Aktivieren des Agent für die Datenbank des Online-Besprechungszentrums (STConf.nsf) auf dem Sametime Server